

## PATENT COOPERATION TREATY

## PCT

NOTICE INFORMING THE APPLICANT OF THE  
COMMUNICATION OF THE INTERNATIONAL  
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira  
No.11 Mori Building  
6-4, Toranomom 2-chome  
Minato-ku  
Tokyo 105-0001  
JAPON

Date of mailing (day/month/year)

05 October 2000 (05.10.00)

Applicant's or agent's file reference

SK00PCT31

## IMPORTANT NOTICE

International application No.

PCT/JP00/02041

International filing date (day/month/year)

30 March 2000 (30.03.00)

Priority date (day/month/year)

30 March 1999 (30.03.99)

Applicant

SONY CORPORATION et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

AG,AU,DZ,KP,KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,  
GE,GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,  
NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on

05 October 2000 (05.10.00) under No. WO 00/58827

## REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a **demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

## REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

J. Zahra

Telephone No. (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-5 relate to an information providing apparatus for receiving a program from a program information processing device over a network, encrypting the received program, and transmitting it to information processing device, to an information providing method, and to a program providing medium.

There is no special technical feature common to the inventions of claims 6-52 and those of claims 1-5.

For example, the inventions of claims 6-8 relate to an information processing apparatus for selecting a mutual authentication to be made from among mutual authentications between information processing devices and carrying out the mutual authentication, to an information processing method, and to a program providing medium.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐

The additional search fees were accompanied by the applicant's protest.

☒

No protest accompanied the payment of additional search fees.

**THIS PAGE BLANK (USPTO)**



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

## A. CLASSIFICATION OF SUBJECT MATTER Int.Cl<sup>7</sup> G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60  
 H04L 9/00-9/32  
 G09C 1/00-5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000  
 Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG (INSPEC): OpenMG, MagicGate, MemoryStick  
 JICST (JOIST) : OpenMG, MagicGate, MemoryStick, Copyright, Contents Down Load

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Taro Yoshio, "Digital Chosakuken:Kogata Memory Card de Chosakuken wo mamoru", <i>Nikkei Electronics</i> , No.739, 22 March, 1999 (Tokyo), p.49-53	1-52
X	Taro Yoshio, "Ongaku Haishin matta nashi: Seibi Isogu Chosakuken Hogo Gijutsu", <i>Nikkei Electronics</i> , No.738, 08 March, 1999 (Tokyo), p.94-98	11-14 1-10,15-52
Y	EP, 875815, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 16 & JP, 10-301772, A	1-5,15-52
Y	EP, 875814, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 22 & JP, 10-301773, A	1-5,15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO.LTD.), 02 September, 1998 (02.09.98), Full text; Figs. 1 to 9 & JP, 10-304333, A	6-8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search  
 21 June, 2000 (21.06.00)

Date of mailing of the international search report  
 04 July, 2000 (04.07.00)

Name and mailing address of the ISA/  
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"DVD, Personal Computer ni noru Software Fukugou no Kagi wo nigiru Fusei Copy Boushi Gijutsu no Medo", <i>Nikkei Electronics</i> , No.696, 18 August, 1997 (Tokyo), p.110-119	9-10, 15-52
Y	David Aucsmith, "Gyaku Kaiseki ya Kaihen kara Soft wo mamoru Tamper Resistant Software Gijutsu no Shousai", <i>Nikkei Electronics</i> , No.706, 05 January, 1998 (Tokyo), p.209-220	9-10, 15-52
Y	EP, 874299, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 32 & JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 41 & JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.), 06 September, 1996 (06.09.96), Full text; Figs. 1 to 87 & JP, 10-512074, A	1-52

PCT

## 国際調査報告

(法8条、法施行規則第40、41条)  
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 SK00PCT31	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JP00/02041	国際出願日 (日.月.年) 30.03.00	優先日 (日.月.年) 30.03.99
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。  
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

## 1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☒ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、  
第 2 図とする。 ☒ 出願人が示したとおりである。

/ ☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

**THIS PAGE BLANK (USPTO)**

## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-5はネットワークを介してプログラムを情報処理装置からプログラムを受信し、受信したプログラムを暗号化して、前記情報処理装置に送信する構成を有する情報提供装置、情報提供方法およびプログラム提供媒体に関するものである。

一方、請求項6-52については上記の構成とは共通の特別な技術的特徴はない。

たとえば、請求の範囲6-8は情報処理装置間の相互認証を行う際において、1以上の相互認証の手続きから、実行する相互認証の処理を選択し、実行する構成を有する情報処理装置、情報処理方法およびプログラム提供媒体に関するものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int Cl<sup>7</sup> G06F9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl<sup>7</sup> G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60  
H04L 9/00~9/32  
G09C 1/00~5/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2000年  
日本国登録実用新案公報 1994-2000年  
日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

DIALOG (INSPEC): OpenMG, MagicGate, MemoryStick

JICST (JOIST): OpenMG, MagicGate, メモリースティック, 著作権, コンテンツ配信

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y ✓	日経エレクトロニクス, 第739号, 22. 3月. 1999 (東京), 芳尾太郎, "デジタル著作権: 小型メモリ・カードで著作権を守る", p. 49-53	1-52
X ✓ Y	日経エレクトロニクス, 第738号, 08. 3月. 1999 (東京), 芳尾太郎, "音楽配信待ったなし・整備急ぐ著作権保護技術", p. 94-98	11-14 1-10, 15-52
Y ✓	EP, 875815, A2 (SONY CORPORATION) 4. 11月. 1998 (04. 11. 98) 全文, 第1~16図 &JP, 10-301772, A	1-5, 15-52

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日 21. 06. 00

国際調査報告の発送日 04.07.00

国際調査機関の名称及びあて先  
日本国特許庁 (ISA/J P)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)  
田川 泰宏

5 B 4 2 3 6

電話番号 03-3581-1101 内線 3545

**THIS PAGE BLANK (USPTO)**



C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y ✓	EP, 875814, A2 (SONY CORPORATION) 4. 11月. 1998 (04. 11. 98) 全文, 第 1 ~ 2 2 図 &JP, 10-301773, A	1-5, 15-52
Y ✓	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.) 2. 9月. 1998 (02. 09. 98) 全文, 第 1 ~ 9 図 &JP, 10-304333, A	6-8
Y ✓	日経エレクトロニクス, 第696号, 18. 8月. 1997 (東京), "DVD、パソコンに載る ソフトウェア復号のカギを握る不正コピー防止技術のメド", p. 110-119	9-10, 15-52
Y ✓	日経エレクトロニクス, 第706号, 05. 1月. 1998 (東京), David Aucsmith, "逆解析や改変からソフトを守る タンパ・レジスタント・ソフトウェア技術の詳細", p. 209-220	9-10, 15-52
Y ✓	EP, 874299, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98) 全文, 第 1 ~ 3 2 図 &JP, 11-53264, A	9-10
Y ✓	EP, 874300, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98) 全文, 第 1 ~ 4 1 図 &JP, 11-53264, A	9-10
A ✓	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.) 6. 9月. 1996 (06. 09. 96) 全文, 第 1 ~ 8 7 図 &JP, 10-512074, A	1-52

**THIS PAGE BLANK (USPTO)**

**THIS PAGE BLANK (USPTO)**

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. cl<sup>7</sup> C02F 3/10, 3/28, 3/06, C12N 11/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. cl<sup>7</sup> C02F 3/10, 3/28, 3/06, C12N 11/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案広報 1926-1996

日本国公開実用新案広報 1971-2000

日本国登録実用新案広報 1994-2000

日本国実用新案登録広報 1996-2000

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI (DIALOG) C02F-003\*magnetic

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 11-18765, A (科学技術振興事業団) 26. 1月. 1999 (26. 01. 99), ファミリーなし	1-3, 5, 7, 10-16
Y	請求項1-3, 【0027】-【0039】, 図1-7	4, 6, 9, 17 8
A		
Y	JP, 3-254895, A (株式会社西原環境衛生研究所) 13. 11月. 1991 (13. 11. 91), ファミリーなし 第2頁右下欄第9-15行	4, 6
Y	JP, 8-257589, A (日本碍子株式会社)	4, 6, 17

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

23. 05. 00

国際調査報告の発送日

30.05.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

吉水 純子

4D

7738

電話番号 03-3581-1101 内線 6425

**THIS PAGE BLANK (USPTO)**

1/5

特許協力条約に基づく国際出願願書

SK00PCT31

副本 - 印刷日時 2000年03月30日 (30. 03. 2000) 木曜日 14時36分01秒

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/R0/101 この特許協力条約に基づく 国際出願願書は、 右記によって作成された。	PCT-EASY Version 2.90 (updated 08.03.2000)
0-5	申立て 出願人は、この国際出願が特許 協力条約に従って処理されるこ とを請求する。	
0-6	出願人によって指定された 受理官庁	日本国特許庁 (R0/JP)
0-7	出願人又は代理人の書類記 号	SK00PCT31
I	発明の名称	情報処理システム
II	出願人	出願人である (applicant only)
II-1	この欄に記載した者は	米国を除くすべての指定国 (all designated States except US)
II-2	右の指定国についての出願人で ある。	ソニー株式会社 SONY CORPORATION 141-0001 日本国 東京都 品川区 北品川 6丁目7番35号 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-4ja	名称	
II-4en	Name	
II-5ja	あて名:	
II-5en	Address:	
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor)
III-1-1	この欄に記載した者は	米国のみ (US only)
III-1-2	右の指定国についての出願人で ある。	石黒 隆二 ISHIGURO, Ryuji 141-0001 日本国 東京都 品川区 北品川 6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-4ja	氏名 (姓名)	
III-1-4en	Name (LAST, First)	
III-1-5ja	あて名:	
III-1-5en	Address:	
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP



**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

III-2 III-2-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor) 米国のみ (US only)
III-2-2	右の指定国についての出願人である。	
III-2-4ja	氏名 (姓名)	河上 達
III-2-4en	Name (LAST, First)	KAWAKAMI, Itaru
III-2-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍 (国名)	日本国 JP
III-2-7	住所 (国名)	日本国 JP
III-3 III-3-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor) 米国のみ (US only)
III-3-2	右の指定国についての出願人である。	
III-3-4ja	氏名 (姓名)	田辺 充
III-3-4en	Name (LAST, First)	TANABE, Mitsuru
III-3-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-3-6	国籍 (国名)	日本国 JP
III-3-7	住所 (国名)	日本国 JP
III-4 III-4-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor) 米国のみ (US only)
III-4-2	右の指定国についての出願人である。	
III-4-4ja	氏名 (姓名)	江面 裕一
III-4-4en	Name (LAST, First)	EZURA, Yuichi
III-4-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-4-6	国籍 (国名)	日本国 JP
III-4-7	住所 (国名)	日本国 JP

**THIS PAGE BLANK (USPTO)**



## 特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年03月30日 (30. 03. 2000) 木曜日 14時36分01秒

III-5 III-5-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor) 米国のみ (US only)
III-5-2	右の指定国についての出願人である。	
III-5-4ja	氏名 (姓名)	河原 博和
III-5-4en	Name (LAST, First)	KAWAHARA, Hirokazu
III-5-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6丁目 7番 35号 ソニー株式会社内
III-5-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-5-6	国籍 (国名)	日本国 JP
III-5-7	住所 (国名)	日本国 JP
IV-1	代理人又は共通の代表者、 通知のあて名 下記の者は国際機関において右 記のごとく出願人のために行動 する。	代理人 (agent)
IV-1-1ja	氏名 (姓名)	小池 晃
IV-1-1en	Name (LAST, First)	KOIKE, Akira
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門二丁目 6番 4号 第11森ビル
IV-1-2en	Address:	No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3508-8266
IV-1-4	ファクシミリ番号	03-3508-0439
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	田村 栄一; 伊賀 誠司
IV-2-1en	Name (s)	TAMURA, Eiichi; IGA, Seiji
V V-1	国の指定 広域特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国で ある他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国 である他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE 及びヨーロッパ特許条約と特許協力条約の締約国 である他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締 約国である他の国

**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年03月30日 (30. 03. 2000) 木曜日 14時36分01秒

V-2	国内特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AE AG AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-5	指定の確認の宣言 出願人は、上記の指定に加えて 、規則4.9(b)の規定に基づき、 特許協力条約のもとで認められ る他の全ての国の指定を行う。 ただし、V-6欄に示した国の指 定を除く。出願人は、これらの 追加される指定が確認を条件と していること、並びに優先日か ら15月が経過する前にその確認 がなされない指定は、この期間 の経過時に、出願人によって取 り下げられたものとみなされる ことを宣言する。	
V-6	指定の確認から除かれる国	なし (NONE)
VI-1	先の国内出願に基づく優先 権主張	
VI-1-1	先の出願日	1999年03月30日 (30. 03. 1999)
VI-1-2	先の出願番号	平成11年特許願第088346号
VI-1-3	国名	日本国 JP
VII-1	特定された国際調査機関 (ISA A)	日本国特許庁 (ISA/JP)
VIII	照合欄	用紙の枚数
VIII-1	願書	5
VIII-2	明細書	117
VIII-3	請求の範囲	19
VIII-4	要約	1
VIII-5	図面	48
VIII-7	合計	190
VIII-8	添付書類	添付
VIII-8	手数料計算用紙	✓
VIII-9	別個の記名押印された委任状	✓
VIII-12	優先権証明書	優先権証明書 VI-1
VIII-16	PCT-EASYディスク	-
VIII-17	その他	納付する手数料に相当す る特許印紙を貼付した書 面
VIII-18	要約書とともに提示する図 の番号	2
VIII-19	国際出願の使用言語名:	日本語 (Japanese)
IX	提出者の記名押印	
IX-1	氏名 (姓名)	
IX-2	権限	

**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

SK00PCT31

副本 - 印刷日時 2000年Q3月30日 (30. 03. 2000) 木曜日 14時36分01秒

## 受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面：	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

## 国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

**THIS PAGE BLANK (USPTO)**



(51) 国際特許分類7  
G06F 9/06

A1

(11) 国際公開番号

WO00/58827

(43) 国際公開日

2000年10月5日(05.10.00)

(21) 国際出願番号

PCT/JP00/02041

(22) 国際出願日

2000年3月30日(30.03.00)

(30) 優先権データ

特願平11/88346

1999年3月30日(30.03.99)

JP

(71) 出願人 (米国を除くすべての指定国について)

ソニー株式会社(SONY CORPORATION)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ)

石黒隆二(ISHIGURO, Ryuji)[JP/JP]

河上 達(KAWAKAMI, Itaru)[JP/JP]

田辺 充(TANABE, Mitsuru)[JP/JP]

江面裕一(EZURA, Yuichi)[JP/JP]

河原博和(KAWAHARA, Hirokazu)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号

ソニー株式会社内 Tokyo, (JP)

(74) 代理人

小池 晃, 外(KOIKE, Akira et al.)

〒105-0001 東京都港区虎ノ門二丁目6番4号

第11森ビル Tokyo, (JP)

(81) 指定国 AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

添付公開書類

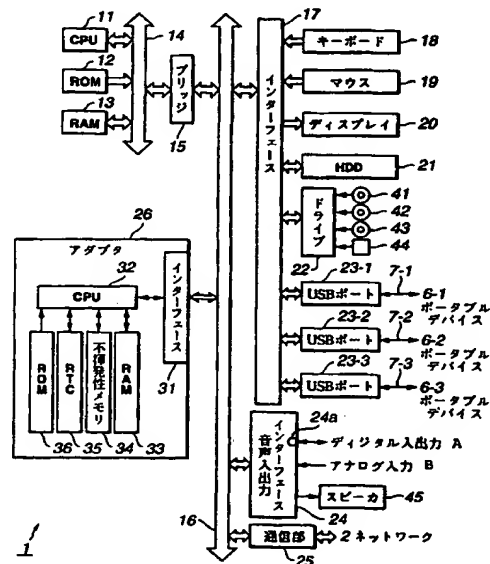
国際調査報告書

(54)Title: INFORMATION PROCESSING SYSTEM

(54)発明の名称 情報処理システム

(57) Abstract

A personal computer (1) transmits a source program to which a signature is attached to an authenticating station through a communication unit (25). The authenticating station, if no alteration is found in the received source program, encrypts the source program with a secret key of the authenticating station, and transmits the encrypted source program to the personal computer (1). The personal computer (1) records the encrypted source program on an HDD (21) and transmits it to an adapter (26).



24a...INTERFACE AUDIO INPUT/OUTPUT  
A...DIGITAL INPUT/OUTPUT  
B...ANALOG INPUT  
45...LOUDSPEAKER  
25...COMMUNICATION UNIT  
2...NETWORK

15...BRIDGE  
26...ADAPTER  
31...INTERFACE  
34...NONVOLATILE MEMORY  
17...KEYBOARD  
18...INTERFACE  
19...MOUSE  
20...DISPLAY

22...DRIVE  
23-1...USB PORT  
23-2...USB PORT  
23-3...USB PORT  
6-1...PORTABLE DEVICE  
6-2...PORTABLE DEVICE  
6-3...PORTABLE DEVICE

パーソナルコンピュータ 1 は、通信部 2 5 を介して、認証局に署名を付したソースプログラムを送信し、認証局は、受信したソースプログラムに改竄が発見されなかった場合、受信したソースプログラムを認証局の秘密鍵で暗号化してパーソナルコンピュータ 1 に送信する。パーソナルコンピュータ 1 は、認証局から受信した暗号化されたソースプログラムを HDD 2 1 に記録するとともにアダプタ 2 6 に送信する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LR	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LV	ラトヴィア	SN	セネガル
BB	バルバドス	GD	グレナダ	MA	モロッコ	SZ	スワジランド
BE	ベルギー	GE	グルジア	MC	モナコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MD	モルドヴァ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MG	マダガスカル	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MK	マケドニア旧ユーゴスラヴィア	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ		共和国	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ	ML	マリ	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	MN	モンゴル	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MR	モーリタニア	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MW	マラウイ	UG	ウガンダ
CH	スイス	IE	アイルランド	MX	メキシコ	US	米国
CI	コートジボアール	IL	イスラエル	MZ	モザンビーク	UZ	ウズベキスタン
CM	カメルーン	IN	インド	NE	ニジェール	VN	ヴェトナム
CN	中国	IS	アイスランド	NL	オランダ	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NZ	ニュージーランド	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	PT	ポルトガル		
CZ	チェコ	KG	キルギスタン	RO	ルーマニア		
DE	ドイツ	KP	北朝鮮				
DK	デンマーク	KR	韓国				



## 明細書

### 情報処理システム

#### 技術分野

本発明は、情報提供装置、情報処理方法及び認証方法、半導体 I C、情報処理システム、並びにプログラム提供媒体に関し、特に、所定のデータを記憶し、所定の処理を行うための情報処理装置、情報処理方法及び認証方法、半導体 I C、情報処理システム、並びにプログラム提供媒体に関する。

#### 背景技術

最近、C D (Compact Disk)、M D (Mini Disk) といった音楽データをデジタル的に記録又は再生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

例えば、コピー元を制御するソフトウェアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

また、コピー元のソフトウェアに所定のハードウェアに記憶されている識別情報IDを利用して、コピー先の装置と相互認証させることも提案されている。

さらにまた、認証、暗号及び復号処理を、ワイアードロジックのハードウェアで実行させることも提案されている。

しかしながら、ソフトウェアだけで認証処理、暗号化処理及び復号処理を行うようにする場合、ソフトウェアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

また、所定のIDをハードウェアに記憶させ、パーソナルコンピュータ上のソフトウェアにより、これを読み出し、利用させるようにする場合、読み出されたIDがソフトウェアに転送される途中において読み取られ、解析、改竄されてしまう恐れがあった。

さらに、認証処理、暗号化処理及び復号処理をワイアードロジックのハードウェアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理及び復号処理を行うようにするには、既存のハードウェアを新たなハードウェアと交換するか、新たなハードウェアを追加する必要が生じる。

本発明は、このような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

すなわち、本発明は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置において、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信手段と、通信手段が受信した前記プログラムを暗号化する暗号化手段とを含むことを特徴とする。

また、本発明は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置の情報提供方法において、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、通信ステップで受信した前記プログラムを暗号化する暗号化ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置に、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、通信ステップで受信した前記プログラムを暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置において、前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択

手段と、前記選択手段が選択された相互認証の手続を実行する相互認証手段とを含むことを特徴とする。

また、本発明は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置の情報処理方法において、前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、前記選択ステップで選択された相互認証の手続を実行する相互認証ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置に、前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、前記選択ステップで選択された相互認証の手続を実行する相互認証ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明に係る認証方法は、第1装置において第1乱数を発生し、第1装置の識別情報と鍵の属性情報と上記第1乱数とを第1装置から第2装置に送信し、第2装置において第2乱数を発生し、第2装置において上記第1装置から送信された第1装置の識別情報と鍵の属性情報と第1乱数とを受信し、第2装置において上記鍵の属性情報から鍵を計算し、第2装置において上記鍵と上記第1・第2乱数から第3乱数を発生し、第2・第3乱数と鍵に関する情報とを第2装置から第1装置に送信し、第1装置において上記第2装置から送信された第2・第3乱数と鍵に関する情報とを受信し、第1装置において上記鍵に関する情報から鍵を生成し、第1装置において上記鍵と上記第1・第2乱数から第4乱数を発生し、上記第4乱

数を第1装置から第2装置に送信し、第1・第2装置の各々において第3・第4乱数と鍵とから一時鍵を求めることを特徴とする。

また、本発明に係る認証方法は、第1装置において第1乱数を発生し、第1装置の識別情報と第1装置の鍵の属性情報と第2装置の鍵の属性情報と上記第1乱数とを第1装置から第2装置に送信し、第2装置において第2乱数を発生し、第2装置において上記第1装置から送信された第1装置の識別情報と鍵の属性情報と第2装置の鍵の属性情報と上記第1乱数とを受信し、第2装置において上記第2装置の鍵の属性情報から第1鍵を計算し、第2装置において上記第1装置の鍵の属性情報から第2鍵を計算し、第2装置において上記第2鍵と上記第1・第2乱数から第3乱数を発生し、第2・第3乱数と鍵に関する情報とを第2装置から第1装置に送信し、第1装置において上記第2装置から送信された第2・第3乱数と鍵に関する情報とを受信し、第1装置において上記鍵に関する情報から第2鍵を生成し、第1装置において上記第2鍵と上記第1・第2乱数から第4乱数を発生し、上記第4乱数を第1装置から第2装置に送信し、第1・第2装置の各々において第3・第4乱数と第2鍵とから一時鍵を求めることを特徴とする。

また、本発明は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置において、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信手段と、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済手段とを含む

ことを特徴とする。

また、本発明は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供方法において、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置に、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明に係る情報処理装置は、暗号化されているプログラムを復号して実行する第1の実行手段と、前記プログラムを前記第1の実行手段に供給するとともに、暗号化されている前記プログラムを復号し、前記第1の実行手段の実行の結果を基に、前記プログラムを実行する第2の実行手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、暗号化されているプログラムを復号して実行する第1の実行ステップと、前記プログラムを前

記第 1 の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第 1 の実行ステップの実行の結果を基に、前記プログラムを実行する第 2 の実行ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、暗号化されているプログラムを復号して実行する第 1 の実行ステップと、前記プログラムを前記第 1 の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第 1 の実行ステップの実行の結果を基に、前記プログラムを実行する第 2 の実行ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを

含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置及び認証局からなる情報処理システムにおいて、前記情報処理装置は、前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含み、前記認証局は、前記半導体 I C に実行させる前記プログラムを受信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段とを含むことを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び



替え手段と、前記命令列が並び替えられた前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記命令列が並び替えられた前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記命令列が並び替えられた前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、前記プログラムを暗号化する暗号化手段と、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記プログラムを暗号化する暗号化ステップと、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記プログラムを暗号化する暗号化ステップと、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体 I C において、前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信手段と、前記受信手段により受信された前記第 1 のプログラムを復号する復号手段と、前記復号手段により復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持手段と、前記保持手段に保持されている前記第 2 のプログラムに基づいて処理された前記第 1 のプログラムを実行する実行手段

と、前記実行手段が実行した結果を前記情報処理装置に転送する転送手段と、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時手段とを含むことを特徴とする。

また、本発明は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体 I C の情報処理方法において、前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信ステップと、前記受信ステップで受信された前記第 1 のプログラムを復号する復号ステップと、前記復号ステップで復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持ステップと、前記保持ステップの処理で保持された前記第 2 のプログラムに基づいて処理された前記第 1 のプログラムを実行する実行ステップと、前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体 IC に、前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信ステップと、前記受信ステップで受信された前記第 1 のプログラムを復号する復号ステップと、前記復号ステップで復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持ステップと、前記保持ステップの処理で保持された前記第 2 のプログラムに基づいて処理された前記第 1 のプログラムを実行する実行ステップと、前記実行ステップの処

理で実行した結果を前記情報処理装置に転送する転送ステップと、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、装着された半導体ICに各種の指令を出力し、実行させる情報処理装置において、前記半導体ICに暗号化されているプログラムを送信する送信手段と、前記半導体ICが、前記プログラムを処理した結果生成し、出力したデータを受信する第1の受信手段と、他の装置からデータと時刻情報を受信する第2の受信手段と、前記第2の受信手段が受信したデータを蓄積する蓄積手段と、前記第2の受信手段が受信した時刻情報に基づいて、前記半導体ICの時刻情報を修正させる修正手段とを含むことを特徴とする。

また、本発明は、装着された半導体ICに各種の指令を出力し、実行させる情報処理装置の情報処理方法において、前記半導体ICに暗号化されているプログラムを送信する送信ステップと、前記半導体ICが、前記プログラムを処理した結果生成し、出力したデータを受信する第1の受信ステップと、他の装置からデータと時刻情報を受信する第2の受信ステップと、前記第2の受信ステップで受信したデータを蓄積する蓄積ステップと、前記第2の受信ステップで受信した時刻情報に基づいて、前記半導体ICの時刻情報を修正させる修正ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、装着された半導体ICに各種の指令を出力し、実行させる情報処理装置に、前記半導体ICに暗号化されているプログラムを送信する送信ステップと、前

記半導体 I C が、前記プログラムを処理した結果生成し、出力したデータを受信する第 1 の受信ステップと、他の装置からデータと時刻情報を受信する第 2 の受信ステップと、前記第 2 の受信ステップで受信したデータを蓄積する蓄積ステップと、前記第 2 の受信ステップで受信した時刻情報に基づいて、前記半導体 I C の時刻情報を修正させる修正ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、所定の半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化手段と、前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化手段とを含むことを特徴とする。

また、本発明は、所定の半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化ステップと、前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、所定の半導体 I C が

装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化ステップと、前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体 I C において、前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第 1 の鍵及び前記情報処理装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成手段と、前記プログラムを第 3 の鍵で復号する第 1 の復号手段と、前記データを第 2 の鍵で復号する第 2 の復号手段とを含むことを特徴とする。

また、本発明は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体 I C の情報処理方法において、前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶ステップと、前記記憶ステップで記憶している前記第 1 の鍵及び前記情報処理装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成ステップと、前記プログラムを第 3 の鍵で復号する第 1 の復号ステップと、前記データを第 2 の鍵で復号する第 2 の

復号ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体 I C に、前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶ステップと、前記記憶ステップで記憶している前記第 1 の鍵及び前記情報処理装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成ステップと、前記プログラムを第 3 の鍵で復号する第 1 の復号ステップと、前記データを第 2 の鍵で復号する第 2 の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

さらに、本発明は、半導体 I C に実行させるプログラムを供給する情報処理装置及び前記情報処理装置に装着され、前記情報処理装置から供給されたプログラムを受信し、前記プログラムを実行する半導体 I C からなる情報処理システムにおいて、前記情報処理装置は、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化手段と、前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化手段と、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記半導体 I C に送信するとともに、前記第 1 の鍵及び前記第 2 の鍵を前記半導体 I C から受信する第 1 の通信手段とを含み、前記半導体 I C は、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記情

報処理装置から受信するとともに、前記第 1 の鍵及び前記第 2 の鍵を前記情報処理装置に送信する第 2 の通信手段と、前記半導体 IC 固有の第 3 の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第 3 の鍵及び前記情報処理装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成手段と、前記第 2 の通信手段が受信した、前記プログラムを第 1 の鍵で復号する第 1 の復号手段と、前記第 2 の通信手段が受信した、前記データを第 2 の鍵で復号する第 2 の復号手段とを含むことを特徴とする。

#### 図面の簡単な説明

図 1 は、本発明を適用したコンテンツデータ管理システムの一実施の形態を示す図である。

図 2 は、上記コンテンツデータ管理システムにおけるパーソナルコンピュータの構成を説明する図である。

図 3 は、コンテンツデータ管理システムにおけるポータブルデバイスの構成を説明する図である。

図 4 は、上記パーソナルコンピュータの機能の構成を説明するブロック図である。

図 5 は、表示操作指示ウィンドウの例を示す図である。

図 6 は、録音プログラムがディスプレイに表示させるウィンドウの例を説明する図である。

図 7 は、コンパクトディスクから HDD にコンテンツをコピーする場合の処理を説明するフローチャートである。



図 8 は、図 7 のフローチャートにおけるステップ S 1 2 の期限データベースチェック処理を説明するフローチャートである。

図 9 は、期限データベースの例を示す図である。

図 1 0 は、ウォータマークを説明する図である。

図 1 1 は、曲データベースの例を示す図である。

図 1 2 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図 1 3 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図 1 4 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図 1 5 は、図 1 2 のフローチャートにおけるステップ S 5 5 の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

図 1 6 は、ポータブルデバイス管理している再生条件を説明する図である。

図 1 7 は、図 1 2 のフローチャートにおけるステップ S 5 8 のフォーマット変換処理の詳細を説明するフローチャートである。

図 1 8 は、H D D からポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図 1 9 は、H D D からポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図 2 0 は、H D D からポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図 2 1 は、ポータブルデバイスから H D D へコンテンツを移動す

る場合の動作を説明するフローチャートである。

図 2 2 は、ポータブルデバイスから H D D へコンテンツをコピーする場合の動作を説明フローチャートである。

図 2 3 は、E M D サーバから H D D へコンテンツをコピーする場合の処理を説明するフローチャートである。

図 2 4 は、図 2 3 のフローチャートにおけるステップ S 2 0 4 の課金に関する処理の詳細を説明するフローチャートである。

図 2 5 は、課金ログを説明する図である。

図 2 6 は、パーソナルコンピュータの I E C 6 0 9 5 8 端子から H D D へコンテンツをコピーする場合の処理を説明するフローチャートである。

図 2 7 は、パーソナルコンピュータの I E C 6 0 9 5 8 端子から H D D へコンテンツをコピーする場合の処理を説明するフローチャートである。

図 2 8 は、H D D から I E C 6 0 9 5 8 端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図 2 9 は、H D D から I E C 6 0 9 5 8 端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 0 は、図 2 8 のフローチャートにおけるステップ S 2 7 5 の再生条件などのチェック処理を説明するフローチャートである。

図 3 1 は、H D D からポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 2 は、H D D からポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 3 は、不揮発性メモリの機能を説明する図である。

図 3 4 は、アダプタの動作を説明するフローチャートである。

図 3 5 は、アダプタの内部の構成を示す図である。

図 3 6 A 及び図 3 6 B は、不揮発性メモリの内部の構成例を示す断面図である。

図 3 7 は、不揮発性メモリの内部の構成例を示す斜視図である。

図 3 8 は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図 3 9 は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図 4 0 は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図 4 1 は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図 4 2 は、ソースプログラムを暗号化する処理を説明するフローチャートである。

図 4 3 は、暗号化されたソースプログラムをアダプタが実行する処理を説明するフローチャートである。

図 4 4 は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

図 4 5 は、暗号化されたオブジェクトプログラムをアダプタが実行する処理を説明するフローチャートである。

図 4 6 は、オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

図 4 7 は、暗号化されたオブジェクトプログラムをアダプタ 7 が実行する他の処理を説明するフローチャートである。

図 4 8 は、アダプタがオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータの CPU に実行させるときの処理を説明するフローチャートである。

図 4 9 は、パーソナルコンピュータが EMD サーバから暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

図 1 は、本発明を適用したコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ 1 は、ローカルエリアネットワーク又はインターネットなどから構成されるネットワーク 2 に接続されている。パーソナルコンピュータ 1 は、EMD (Electrical Music Distribution) サーバ 4-1 乃至 4-3 から受信した、又は後述する CD (Compact Disc) から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC 3（商標））に変換するとともに DES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

利用条件のデータは、例えば、その利用条件のデータに対応する

コンテンツを同時に利用することができるポータブルデバイス(Portable Device(PDとも称する))の台数(後述する、いわゆるチェックアウトできるPDの台数)を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ1は、そのコンテンツを再生できる。

又は、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス6-1乃至6-3にコピーしたとき、パーソナルコンピュータ1は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス6-1乃至6-3に記憶させることができる回数は、制限される場合がある。この場合、コピーできる回数は、増えることがない。

又は、利用条件のデータは、他のパーソナルコンピュータに移動することができるなどを示す。ポータブルデバイス6-1乃至6-3にコンテンツを移動させた後、パーソナルコンピュータ1が記録しているコンテンツは使用できなくなる(コンテンツが削除されるか、又は利用条件が変更されて使用できなくなる)。

利用条件のデータの詳細は、後述する。

パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ(例えば、曲名、又は再生条件など)とともに、USB(Universal Serial Bus)ケーブル7-1を介して、接続されているポータブルデバイス6-1に記憶させるとともに、ポータブルデバイス6-1に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する(以下、チェックアウトと称する)。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテン

ツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、USBケーブル7-2を介して、接続されているポータブルデバイス6-2に記憶させるとともに、ポータブルデバイス6-2に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、USBケーブル7-3を介して、接続されているポータブルデバイス6-3に記憶させるとともに、ポータブルデバイス6-3に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

また、パーソナルコンピュータ1は、USBケーブル7-1を介して、接続されているポータブルデバイス6-1にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-1に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ1が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1増やされる。

パーソナルコンピュータ1は、USBケーブル7-2を介して、接続されているポータブルデバイス6-2にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-2に消去させて（又は、使用できなくさせて）、消去させたコンテ

ンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、USB ケーブル 7-3 を介して、接続されているポータブルデバイス 6-3 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6-3 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

パーソナルコンピュータ 1 は、図示せぬ他のパーソナルコンピュータがポータブルデバイス 6-1 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6-2 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6-3 にチェックアウトしたコンテンツをチェックインできない。

EMD 登録サーバ 3 は、パーソナルコンピュータ 1 が EMD サーバ 4-1 乃至 4-3 からコンテンツの取得を開始するとき、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、パーソナルコンピュータ 1 と EMD サーバ 4-1 乃至 4-3 との相互認証に必要な認証鍵をパーソナルコンピュータ 1 に送信するとともに、EMD サーバ 4-1 乃至 4-3 に接続するためのプログラムをパーソナルコンピュータ 1 に送信する。

EMD サーバ 4-1 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに、パーソナルコンピュータ 1 にコンテンツを供給する。EMD サーバ 4-2 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コン

テンツに関連するデータとともに、パーソナルコンピュータ 1 にコンテンツを供給する。EMDサーバ 4-3 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ 1 にコンテンツを供給する。

EMDサーバ 4-1 乃至 4-3 のそれぞれが供給するコンテンツは、同一又は異なる圧縮の方式で圧縮されている。EMDサーバ 4-1 乃至 4-3 のそれぞれが供給するコンテンツは、同一又は異なる暗号化の方式で暗号化されている。

WWW(World Wide Web)サーバ 5-1 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD (例えば、CD のアルバム名、又は CD の販売会社など) 及び CD から読み取ったコンテンツに対応するデータ (例えば、曲名、又は作曲者名など) をパーソナルコンピュータ 1 に供給する。WWWサーバ 5-2 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD 及び CD から読み取ったコンテンツに対応するデータをパーソナルコンピュータ 1 に供給する。

ポータブルデバイス 6-1 は、パーソナルコンピュータ 1 から供給されたコンテンツ (すなわち、チェックアウトされたコンテンツ) を、コンテンツに関連するデータ (例えば、曲名、又は再生制限など) とともに記憶する。ポータブルデバイス 6-1 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

例えば、コンテンツに関連するデータとして記憶されている、再



再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。

使用者は、コンテンツを記憶したポータブルデバイス 6-1 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-2 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-2 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-2 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-3 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-3 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-3 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

以下、ポータブルデバイス 6-1 乃至 6-3 を個々に区別する必要がないとき、単にポータブルデバイス 6 と称する。

図 2 は、パーソナルコンピュータ 1 の構成を説明する図である。CPU (Central Processing Unit) 11 は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System) を実際に実行する。ROM (Read-only Memory) 12 は、一般的には、CPU 11 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 13 は、CPU 11 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらは CPU バスなどから構成されるホストバス 14 により相互に接続されている。

ホストバス 14 は、ブリッジ 15 を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス 16 に接続されている。

キーボード 18 は、CPU 11 に各種の指令を入力するとき、使用者により操作される。マウス 19 は、ディスプレイ 20 の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 20 は、液晶表示装置又は CRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21 は、ハードディスクを駆動し、それらに CPU 11 によって実行するプログラムや情報を記録又は再生させる。

ドライブ 22 は、装着されている磁気ディスク 41、光ディスク 42 (CD を含む)、光磁気ディスク 43、又は半導体メモリ 44 に記録されているデータ又はプログラムを読み出して、そのデータ

又はプログラムを、インターフェース 17、外部バス 16、ブリッジ 15 及びホストバス 14 を介して接続されている RAM 13 に供給する。

USB ポート 23-1 には、USB ケーブル 7-1 を介して、ポータブルデバイス 6-1 が接続される。USB ポート 23-1 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-1 のコマンドなどを含む）をポータブルデバイス 6-1 に出力する。

USB ポート 23-2 には、USB ケーブル 7-2 を介して、ポータブルデバイス 6-2 が接続される。USB ポート 23-2 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-2 のコマンドなどを含む）をポータブルデバイス 6-2 に出力する。

USB ポート 23-3 には、USB ケーブル 7-3 を介して、ポータブルデバイス 6-3 が接続される。USB ポート 23-3 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-3 のコマンドなどを含む）をポータブルデバイス 6-3 に出力する。

I E C (International Electrotechnical Commission) 6 0 9 5 8

端子 2 4 a を有する音声入出力インターフェース 2 4 は、デジタル音声入出力、あるいはアナログ音声入出力のインターフェース処理を実行する。スピーカ 4 5 は、音声入出力インターフェース 2 4 から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

これらのキーボード 1 8 乃至音声入出力インターフェース 2 4 は、インターフェース 1 7 に接続されており、インターフェース 1 7 は、外部バス 1 6、ブリッジ 1 5 及びホストバス 1 4 を介して CPU 1 1 に接続されている。

通信部 2 5 は、ネットワーク 2 が接続され、CPU 1 1、又は HDD 2 1 から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式の packets に格納して、ネットワーク 2 を介して、送信するとともに、ネットワーク 2 を介して、受信した packets に格納されているデータ（例えば、認証鍵、又はコンテンツなど）を CPU 1 1、RAM 1 3、又は HDD 2 1 に出力する。

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 2 6 の CPU 3 2 は、外部バス 1 6、ブリッジ 1 5 及びホストバス 1 4 を介してパーソナルコンピュータ 1 の CPU 1 1 と共働し、各種の処理を実行する。RAM 3 3 は、CPU 3 2 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 3 4 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 3 6 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記

憶されている。R T C (Real Time Clock) 35は、計時動作を実行し、時刻情報を提供する。

通信部25及びアダプタ26は、外部バス16、ブリッジ15及びホストバス14を介してCPU11に接続されている。

以下、USBポート23-1乃至23-3を個々に区別する必要がないとき、単に、USBポート23と称する。以下、USBケーブル7-1乃至7-3を個々に区別する必要がないとき、単にUSBケーブル7と称する。

次に、ポータブルデバイス6の構成を図3を参照して説明する。電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU53乃至表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1から転送されたコンテンツを含むデータを、内部バス58を介して、CPU53に供給する。

パーソナルコンピュータ1から転送されるデータは、1パケット当たり64バイトのデータから構成され、12Mbit/secの転送レートでパーソナルコンピュータ1から転送される。

ポータブルデバイス6に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されているとともに、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限及び再生回数カウンタなどが格納されている。コンテンツは、ATRAC3などの

符号化方式で符号化され、暗号化されている。

ヘッダサイズは、ヘッダのデータ長（例えば、33バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、33,636,138バイトなど）を表す。

コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ1とポータブルデバイス6との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ1からポータブルデバイス6に送信される。

ポータブルデバイス6がUSBケーブル7を介してパーソナルコンピュータ1のUSBポート23に接続されたとき、ポータブルデバイス6とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス6のDSP59は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ1が生成するある値（チャレンジ）に対して、ポータブルデバイス6がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ1が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス6が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナル

コンピュータ 1 は不正を検出できる。

コンテンツ ID は、コンテンツに対応した、コンテンツを特定するための ID である。

コーデック ID は、コンテンツの符号化方式に対応した ID であり、例えば、コーデック ID " 1 " は、A T R A C 3 に対応し、コーデック ID " 0 " は、M P 3 (MPEG(Moving Picture Experts Group) Audio Layer-3) に対応する。

ファイル名は、コンテンツに対応するパーソナルコンピュータ 1 が記録しているコンテンツファイル（後述する）を A S C I I (American National Standard Code for Information Interchange) コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などを A S C I I コードに変換したデータである。

再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時又は終了日時）又は回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、" 1 " が割り当てられ、再生が可能な期間が設定されているとき、" 2 " が割り当てられ、回数制限及び再生が可能な期間がいずれも設定されていないとき（いわゆる、買取りで購入されたとき）、" 0 " が割り当てられる。

開始日時及び終了日時は、再生制限データが " 2 " であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が " 0 0 4 0 F " であり、終了日時が " 0 0 0 7 0 F " であるとき、対応するコンテンツは、2 0 0 0 年 4 月 1 5 日から 2 0 0 0 年 7 月 1 5 日まで、再生が可能である。

同様に、回数制限及び再生回数カウンタは、再生制限データが” 1 ” 又は ” 2 ” であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU 53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が” 0 2 ” であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが” 0 1 ” であるとき、そのコンテンツが再生された回数は1回である。

例えば、再生制限データが” 2 ” であり、開始日時が” 0 0 0 4 0 F ” であり、終了日時が” 0 0 0 7 0 F ” であり、回数制限が” 0 2 ” であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間において、1日2回ずつ繰り返し再生できる。

例えば、再生制限データが” 1 ” であり、開始日時が” 0 0 0 0 0 0 ” であり、終了日時が” 0 0 0 0 0 0 ” であり、回数制限が” 0 a ” であり、再生回数カウンタが” 0 5 ” であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツとともにコンテンツの書き込み命令を受信した場合、ROM 55からRAM 54に読み出したメインプログラムを実行するCPU 53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

フラッシュメモリ61は、約64MByteの記憶容量を有し、



コンテンツを記憶する。また、フラッシュメモリ 61 には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

なお、フラッシュメモリ 61 は、ポータブルデバイス 6 にメモリカードとして着脱可能とすることができる。

使用者による、図示せぬ再生／停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ 62 を介して CPU 53 に供給されると、CPU 53 は、フラッシュメモリコントローラ 60 に、フラッシュメモリ 61 から、再生用コードとコンテンツとを読み出させ、DSP 59 に転送させる。

DSP 59 は、フラッシュメモリ 61 から転送された再生用コードに基づいてコンテンツを CRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ（図 3 中において D1 で示す）をデジタル／アナログ変換回路 63 に供給する。

DSP 59 は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子 59A からのマスタークロック MCLK を基に、コンテンツを再生するとともに、マスタークロック MCLK、マスタークロック MCLK を基に内部の発振回路で生成した所定の周波数のビットクロック BCLK、並びに、フレーム単位の L チャンネルクロック LCLK 及び R チャンネルクロック RCLK からなる動作クロック LRCLK をデジタルアナログ変換回路 63 に供給する。

DSP 59 は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路 63 に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロ

ックの供給を停止して、ディジタルアナログ変換回路 6 3 を停止させて、ポータブルデバイス 6 全体の消費電力量を低減する。

同様に、CPU 5 3 及び USB コントローラ 5 7 も、水晶でなる発振子 5 3 A 又は 5 7 A がそれぞれ外付けされ、発振子 5 3 A 又は 5 7 A からそれぞれ供給されるマスタークロック MCLK に基づき、所定の処理を実行する。

このように構成することで、ポータブルデバイス 6 は、CPU 5 3、DSP 5 9、USB コントローラ 5 7 等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

ディジタルアナログ変換回路 6 3 は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路 6 4 に供給する。増幅回路 6 4 は、音声信号を増幅して、ヘッドフォンジャック 6 5 を介して、図示せぬヘッドフォンに音声信号を供給する。

このように、ポータブルデバイス 6 は、図示せぬ再生／停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいてフラッシュメモリ 6 1 に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

ポータブルデバイス 6 は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6 は、自動的に電源をオフして消費電力を低減する。

因みに、ポータブルデバイス 6 は、電源がオフになった後に再生

／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1曲目から再生する。

また、ポータブルデバイス6のCPU53は、LCDコントローラ68を制御して、表示部67に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池51の残量等の情報を表示させる。

さらに、ポータブルデバイス6は、EEPROM68に、フラッシュメモリ80に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ61のブロック位置及びその他種々のメモリ蓄積情報等のいわゆるFAT（File Allocation Table）を格納する。

因みに、本実施の形態においては、コンテンツは、64KByteを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がFATに格納される。

フラッシュメモリ61にFATが格納される場合、例えば、1曲目のコンテンツがCPU53の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

このように、FATは、フラッシュメモリ61へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一の

データがリザーブ用に2重に書き込まれる。

FATがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書換えの回数に達してしまい、フラッシュメモリ61の書換えができなくなってしまう。

そこで、ポータブルデバイス6は、FATをEEPROM68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書換えの頻度を少なくしている。

書換えの回数の多いFATをEEPROM68に記憶させることにより、FATをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU53は、EEPROM68にFATを追記するように書き込ませるので、EEPROM68の同一の領域の書換えの頻度を少なくして、EEPROM68が短期間で書換え不能になることを防止する。

ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

CPU53は、USB接続されたとき、DSP59のコンテンツ

の再生の処理を停止させる。これにより、CPU 53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

このようにCPU 53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

なお、CPU 53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP 59の再生処理を停止させることにより、DSP 59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

図4は、CPU 11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、暗号方式変換プログラム135、圧縮方式変換プログラム136、暗号化プログラム137、利用条件変換プログラム139、利用条件管理プログラム140、認証プログラム141、復号プログラム142、PD用ドライバ143、購入用プログラム144及び購入用プログラム145などの複数のプログラムで構成されている。

コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクショ

ンなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム 1 1 1 を読み出しても、インストラクションを特定できないなど）ように構成されている。

EMD 選択プログラム 1 3 1 は、コンテンツ管理プログラム 1 1 1 がパーソナルコンピュータ 1 にインストールされる時、コンテンツ管理プログラム 1 1 1 には含まれず、後述する EMD の登録の処理において、ネットワーク 2 を介して、EMD 登録サーバ 3 から受信される。EMD 選択プログラム 1 3 1 は、EMD サーバ 4 - 1 乃至 4 - 3 のいずれかとの接続を選択して、購入用アプリケーション 1 1 5、又は購入用プログラム 1 4 4 若しくは 1 4 2 に、EMD サーバ 4 - 1 乃至 4 - 3 のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

チェックイン／チェックアウト管理プログラム 1 3 2 は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に基づいて、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトするか、又はポータブルデバイス 6 - 1 乃至 6 - 3 に記憶されているコンテンツをチェックインする。

チェックイン／チェックアウト管理プログラム 1 3 2 は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータを更新する。

コピー管理プログラム 1 3 3 は、コンテンツデータベース 1 1 4

に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に基づいて、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにコピーするか、又はポータブルデバイス 6 - 1 乃至 6 - 3 からコンテンツをコンテンツデータベース 1 1 4 にコピーする。

移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に基づいて、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに移動するか、又はポータブルデバイス 6 - 1 乃至 6 - 3 からコンテンツをコンテンツデータベース 1 1 4 に移動する。

暗号方式変換プログラム 1 3 5 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの暗号化の方式、購入用プログラム 1 4 4 が EMD サーバ 4 - 2 から受信したコンテンツの暗号化の方式、又は購入用プログラム 1 4 5 が EMD サーバ 4 - 3 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式に変換する。

また、暗号方式変換プログラム 1 3 5 は、ポータブルデバイス 6 - 1 又は 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 又は 6 - 3 が利用可能な暗号化方式に変換する。

圧縮方式変換プログラム 1 3 6 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から

受信したコンテンツの圧縮の方式、購入用プログラム 1 4 4 が E M D サーバ 4 - 2 から受信したコンテンツの圧縮の方式、又は購入用プログラム 1 4 5 が E M D サーバ 4 - 3 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の圧縮の方式に変換する。

また、圧縮方式変換プログラム 1 3 6 は、ポータブルデバイス 6 - 1 又は 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 又は 6 - 3 が利用可能な圧縮の方式に変換する。

暗号化プログラム 1 3 7 は、例えば C D から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

圧縮／伸張プログラム 1 3 8 は、例えば C D から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム 1 3 8 は、符号化されているコンテンツを伸張（復号）する。

利用条件変換プログラム 1 3 9 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が E M D サーバ 4 - 1 から受信したコンテンツの利用条件を示すデータ（いわゆる、U s a g e R u l e）、購入用プログラム 1 4 4 が E M D サーバ 4 - 2 か



ら受信したコンテンツの利用条件を示すデータ、又は購入用プログラム145がEMDサーバ4-3から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース114が記録している利用条件ファイル162-1乃至162-Nに格納されている利用条件データと同一のフォーマットに変換する。

また、利用条件変換プログラム139は、ポータブルデバイス6-1又は6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス6-1又は6-3が利用可能な利用条件のデータに変換する。

利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

認証プログラム141は、コンテンツ管理プログラム111と購入用アプリケーションプログラム115との相互認証の処理及びコンテンツ管理プログラム111と購入用プログラム144との相互認証の処理を実行する。また、認証プログラム141は、EMDサーバ4-1と購入用アプリケーションプログラム115との相互認

証の処理、E M Dサーバ4-2と購入用プログラム144との相互認証の処理及びE M Dサーバ4-3と購入用プログラム145との相互認証の処理で利用される認証鍵を記憶している。

認証プログラム141が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされたとき、認証プログラム141に記憶されておらず、表示操作指示プログラム112により登録の処理が正常に実行されたとき、E M D登録サーバ3から供給され、認証プログラム141に記憶される。

復号プログラム142は、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツをパーソナルコンピュータ1が再生するとき、コンテンツを復号する。

P D用ドライバ143は、ポータブルデバイス6-2に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-2から所定のコンテンツをチェックインするとき、ポータブルデバイス6-2にコンテンツ又はポータブルデバイス6-2に所定の処理を実行させるコマンドを供給する。

P D用ドライバ143は、ポータブルデバイス6-1に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-1から所定のコンテンツをチェックインするとき、デバイスドライバ116-1にコンテンツ、又はデバイスドライバ116-1に所定の処理を実行させるコマンドを供給する。

P D用ドライバ143は、ポータブルデバイス6-3に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-

3から所定のコンテンツをチェックインするとき、デバイスドライバ116-2にコンテンツ、又はデバイスドライバ116-2に所定の処理を実行させるコマンドを供給する。

購入用プログラム144は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム111とともにインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCDに記録されて供給される。購入用プログラム144は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

購入用プログラム144は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム144を読み出しても、インストラクションを特定できないなど）ように構成されている。

購入用プログラム144は、ネットワーク2を介して、EMDサーバ4-2に所定のコンテンツの送信を要求するとともに、EMDサーバ4-2からコンテンツを受信する。また、購入用プログラム144は、EMDサーバ4-2からコンテンツを受信するとき、課金の処理を実行する。

購入用プログラム145は、コンテンツ管理プログラム111とともにインストールされるプログラムであり、ネットワーク2を介して、EMDサーバ4-3に所定のコンテンツの送信を要求するとともに、EMDサーバ4-3からコンテンツを受信する。また、購

入用プログラム145は、EMDサーバ4-3からコンテンツを受信するとき、課金の処理を実行する。

表示操作指示プログラム112は、フィルタリングデータファイル181、表示データファイル182、画像ファイル183-1乃至183-K、又は履歴データファイル184を基に、ディスプレイ20に所定のウィンドウの画像を表示させ、キーボード18又はマウス19への操作を基に、コンテンツ管理プログラム111にチェックイン又はチェックアウトなどの処理の実行を指示する。

フィルタリングデータファイル181は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD21に記録されている。

表示データファイル182は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツに対応するデータを格納して、HDD21に記録されている。

画像ファイル183-1乃至183-Kは、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに対応する画像、又は後述するパッケージに対応する画像を格納して、HDD21に記録されている。

以下、画像ファイル183-1乃至183-Kを個々に区別する必要がないとき、単に、画像ファイル183と称する。

履歴データファイル184は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツがチェックアウトされた回数、チェックイ

ンされた回数、その日付などの履歴データを格納して、HDD 21 に記録されている。

表示操作指示プログラム 112 は、登録の処理のとき、ネットワーク 2 を介して、EMD 登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 111 の ID を送信するとともに、EMD 登録サーバ 3 から認証用鍵及び EMD 選択プログラム 131 を受信して、コンテンツ管理プログラム 111 に認証用鍵及び EMD 選択プログラム 131 を供給する。

録音プログラム 113 は、所定のウィンドウの画像を表示させて、キーボード 18 又はマウス 19 への操作を基に、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツの録音時間などのデータを読み出す。

録音プログラム 113 は、CD に記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWW サーバ 5-1 又は 5-2 に CD に対応するデータ（例えば、アルバム名、又はアーティスト名など）又は CD に記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWW サーバ 5-1 又は 5-2 から CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを受信する。

録音プログラム 113 は、受信した CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを、表示操作指示プログラム 112 に供給する。

また、録音の指示が入力されたとき、録音プログラム 113 は、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツを読み出して、コンテンツ管理プログラム 111 に出力する。

コンテンツデータベース 114 は、コンテンツ管理プログラム 111 から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル 161-1 乃至 161-N のいずれかに格納する（HDD 21 に記録する）。コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N にそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル 161-1 乃至 161-N にそれぞれ対応する利用条件ファイル 162-1 乃至 162-N のいずれかに格納する（HDD 21 に記録する）。

コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N 又は利用条件ファイル 162-1 乃至 162-N をレコードとして記録してもよい。

例えば、コンテンツファイル 161-1 に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-1 に格納されている。コンテンツファイル 161-N に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-N に格納されている。

なお、利用条件ファイル 162-1 乃至 162-N に記録されているデータは、後述する期限データベースに記録されているデータ、又は曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース 114 は、後述する期限データベース及び曲データベースを包含して、構成されている。

以下、コンテンツファイル 161-1 乃至 161-N を個々に区別する必要がないとき、単に、コンテンツファイル 161 と称する。以下、利用条件ファイル 162-1 乃至 162-N を個々に区別す

る必要がないとき、単に、利用条件ファイル 1 6 2 と称する。

購入用アプリケーションプログラム 1 1 5 は、EMD 登録サーバ 3 からネットワーク 2 を介して供給され、又は所定の CD-ROM に記録されて供給される。購入用アプリケーションプログラム 1 1 5 は、ネットワーク 2 を介して、EMD サーバ 4-1 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-1 からコンテンツを受信して、コンテンツ管理プログラム 1 1 1 に供給する。また、購入用アプリケーションプログラム 1 1 5 は、EMD サーバ 4-1 からコンテンツを受信するとき、課金の処理を実行する。

次に、表示データファイル 8 2 に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル 1 6 1-1 乃至 1 6 1-N との対応付けについて説明する。

コンテンツファイル 1 6 1-1 乃至 1 6 1-N のいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

オリジナルパッケージは、1 以上のコンテンツが属し、EMD サーバ 4-1 乃至 4-3 におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚の CD に対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

マイセレクトパッケージは、使用者が任意に選択した 1 以上のコ

ンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ4-1乃至4-3又はWWWサーバ5-1若しくは5-2などからネットワーク2を介して供給され、又は所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ1は、今週の日本のポップス1位のコンテンツ乃至今週の日本のポップス10位のコンテンツを特定することができる。

フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

このようにフィルタリングパッケージのコンテンツは、コンテン



ツに対応するコンテンツ用表示データ 2 2 1 (コンテンツ用表示データ 2 2 1 に使用者が設定したデータを含む)、又は履歴データ 1 8 4 などと、フィルタリングデータとを対応させて選択される。

ドライバ 1 1 7 は、コンテンツ管理プログラム 1 1 1 などの制御の基に、音声入出力インターフェース 2 4 を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム 1 1 1 に供給するか、若しくはコンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 から供給されたコンテンツに対応するアナログ信号を出力する。

図 5 は、表示操作指示プログラム 1 1 2 を起動させたとき、操作指示プログラム 1 1 2 がディスプレイ 2 0 に表示させる表示操作指示ウィンドウの例を示す図である。

表示操作指示ウィンドウには、録音プログラム 1 1 3 を起動させるためのボタン 2 0 1、EMD 選択プログラム 1 3 1 を起動させるためのボタン 2 0 2、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン 2 0 3、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン 2 0 4 等が配置されている。

ボタン 2 0 5 が選択されているとき、フィールド 2 1 1 には、オリジナルパッケージに対応するデータが表示される。ボタン 2 0 6 が選択されているとき、フィールド 2 1 1 には、マイセレクトパッケージに対応するデータが表示される。ボタン 2 0 7 が選択されているとき、フィールド 2 1 1 には、フィルタリングパッケージに対

応するデータが表示される。

フィールド 2 1 1 に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

例えば、図 5 においては、パッケージ名称”ファースト”及びアーティスト名”A 太郎”、パッケージ名称”セカンド”及びアーティスト名”A 太郎”などがフィールド 2 1 1 に表示される。

フィールド 2 1 2 には、フィールド 2 1 1 で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド 2 1 2 に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

例えば、図 5 においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、8 分音符の 1 つがチェックアウト 1 回に相当し、8 分音符が 2 つでチェックアウト 2 回を示す）、並びに曲名”北の墓場”及びチェックアウト可能回数（8 分音符が 1 つでチェックアウト 1 回を示す）などがフィールド 2 1 2 に表示される。

このように、フィールド 2 1 2 に表示されるチェックアウト可能回数としての 1 つの 8 分音符は、対応するコンテンツが 1 回チェックアウトできることを示す。

フィールド 2 1 2 に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が 0 である。（ただし、パーソナルコンピュータ 1

はそのコンテンツを再生することができる。) ) ことを示す。また、フィールド 2 1 2 に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

なお、チェックアウト可能回数は、図 5 に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等でも表示してもよい。

また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図 4 の画像ファイル 1 8 3 - 1 乃至 1 8 3 - K のいずれかに対応する）を表示させるフィールド 2 0 8 が配置されている。ボタン 2 0 9 は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ 4 5 に出力させる）とき、クリックされる。

ボタン 2 0 5 が選択され、フィールド 2 1 1 に、オリジナルパッケージに対応するデータが表示されている場合、フィールド 2 1 2 に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 に、選択されている曲名に対応する、コンテンツデータベース 1 1 4 に格納されている所定のコンテンツを消去させる。

録音プログラム 1 1 3 が表示させるウィンドウのボタン（後述するボタン 2 5 5）が選択されて（アクティブにされて）いる場合、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに記憶されているコンテンツの曲名を表示するフ

フィールド 2 1 3 を表示する。

録音プログラム 1 1 3 が表示させるウィンドウのボタンが選択されている場合、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 に、コンテンツデータベース 1 1 4 に記録した、CD から読み出したコンテンツを予め指定されているポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトさせる。

フィールド 2 1 3 にはコンテンツの曲名に対応させて、フィールド 2 1 3 の最も左に、そのコンテンツがパーソナルコンピュータ 1 にチェックインできるか否かを示す記号が表示される。例えば、フィールド 2 1 3 の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできる（すなわち、パーソナルコンピュータ 1 からチェックアウトされた）ことを示している。フィールド 2 1 3 の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできない（すなわち、パーソナルコンピュータ 1 からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに記憶されているコンテンツが属するパッケージ）の名称

を表示するフィールド 2 1 4、フィールド 2 1 3 を閉じるためのボタン 2 1 0 及びチェックイン又はチェックアウトを実行させるボタン 2 1 5 を表示する。

更に、表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、フィールド 2 1 2 で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン 2 1 6、フィールド 2 1 3 で選択された曲名に対応するコンテンツのチェックインを設定するボタン 2 1 7、フィールド 2 1 3 に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン 2 1 8 及びチェックイン又はチェックアウトの設定を取り消すボタン 2 1 9 を配置させる。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ 1 は、チェックイン又はチェックアウトの処理を実行しない。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定をした後、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム 1 1 1 に、ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかが記憶している所定のコンテンツを消去させるコマン

ドなど)を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル162に格納されている利用条件のデータを更新させる。

チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム112は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル184に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス6-1乃至6-3の名称などから成る。

チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体(設定及び実行を含む)を短くすることができる。

図6は、録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。例えば、WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド251に、“アシンクロナイズド”などのCDのタイトルを表示する。WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド252に、例えば、“クワイ”などのアーティスト名を表示する。

WWWサーバ5-2から受信したCDの情報を基に、録音プログ

ラム 1 1 3 は、フィールド 2 5 3 の曲名を表示する部分に、例えば、” ヒート” , ” プラネット” , ” ブラック” , ” ソウル” などの曲名を表示する。同様に、録音プログラム 1 1 3 は、フィールド 2 5 3 のアーティストを表示する部分に、例えば、” クワイ” などのアーティスト名を表示する。

録音プログラム 1 1 3 が所定の C D の情報を受信した後、録音プログラム 1 1 3 は、H D D 2 1 の所定のディレクトリに C D の情報を格納する。

ボタン 2 5 4 などがクリックされて、C D の情報の取得の指示を受けたとき、録音プログラム 1 1 3 は、始めに、H D D 2 1 の所定のディレクトリを検索する。録音プログラム 1 1 3 は、そのディレクトリに C D の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている C D の情報を利用するか否かを選択させる。

録音プログラム 1 1 3 が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン 2 5 6 がクリックされたとき、録音プログラム 1 1 3 は、ドライブ 2 2 に格納されている C D からコンテンツを読み出して、C D から読み出したコンテンツを C D の情報とともにコンテンツ管理プログラム 1 1 1 に供給する。コンテンツ管理プログラム 1 1 1 の圧縮／伸張プログラム 1 3 8 は、録音プログラム 1 1 3 から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム 1 3 7 は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム 1 3 9 は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

コンテンツ管理プログラム 1 1 1 は、圧縮され、暗号化されたコンテンツを利用条件のデータとともに、コンテンツデータベース 1 1 4 に供給する。

コンテンツデータベース 1 1 4 は、コンテンツ管理プログラム 1 1 1 から受信したコンテンツに対応するコンテンツファイル 1 6 1 及び利用条件ファイル 1 6 2 を生成して、コンテンツファイル 1 6 1 にコンテンツを格納するとともに、利用条件ファイル 1 6 2 に利用条件のデータを格納する。

コンテンツ管理プログラム 1 1 1 は、コンテンツデータベース 1 1 4 にコンテンツ及びコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム 1 1 3 から受信した CD の情報及び利用条件のデータを表示操作指示プログラム 1 1 2 に供給する。

表示操作指示プログラム 1 1 2 は、録音の処理でコンテンツデータベース 1 1 4 に格納されたコンテンツに対応する利用条件のデータ及び CD の情報を基に、表示データファイル 1 8 2 に格納する表示用のデータを生成する。

録音プログラム 1 1 3 が表示させるウィンドウには、更に、CD から読み出したコンテンツをコンテンツデータベース 1 1 4 に記録したとき、自動的に、CD から読み出したコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトさせるか否かの設定を行うボタン 2 5 5 が配置されている。

例えば、ボタン 2 5 5 がクリックされたとき、録音プログラム 1 1 3 は、ポータブルデバイス 6 - 1 乃至 6 - 3 のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかを選択したとき、



パーソナルコンピュータ 1 は、選択されたポータブルデバイス 6-1 乃至 6-3 のいずれかに、自動的に、CD から記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ 1 は、CD からコンテンツを記録したとき、チェックアウトしない。

このように、録音プログラム 113 が表示させるウィンドウのボタン 255 をアクティブにしておくだけで、CD から読み出したコンテンツがコンテンツデータベース 114 に記録されたとき、パーソナルコンピュータ 1 は、予め指定されているポータブルデバイス 6-1 乃至 6-3 のいずれかに、CD から読み出したコンテンツをチェックアウトさせることができる。

次に、図 7 のフローチャートを参照して、コンテンツ管理プログラム 111、表示操作指示プログラム 112、録音プログラム 113、及びコンテンツデータベース 114 を実行する CPU 11 による、ドライブ 22 に装着された CD から再生したコンテンツを HDD 21 に転送し、コピーする場合の処理について説明する。使用者がキーボード 18 又はマウス 19 を操作して、インターフェース 17 を介して CPU 11 に対してドライブ 22 に装着された CD (図示せず) から再生されたコンテンツを HDD 21 に転送、コピーする指令を入力すると、録音プログラム 113 は、ステップ S11 において、インターフェース 17 を介してディスプレイ 20 にコピーするコンテンツを選択するための、例えば、図 6 に示す GUI (Graphical User Interface) を表示させる。

具体的には、例えば、録音プログラム 113 は、ドライブ 22 に

装着されたCDのTOC(Table Of Contents)を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ20に表示させる。又は、録音プログラム113は、CDに含まれている各コンテンツ毎のISRC(International Standard Recording Code)を読み出し、そのコンテンツの情報を得て、ディスプレイ20に表示させる。あるいはまた、ボタン254がクリックされたとき、録音プログラム113は、ネットワーク2を介してWWWサーバ5-1又は5-2にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド253に表示させる。

使用者は、ディスプレイ20のGUIを利用してキーボード18又はマウス19を操作し、フィールド253に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

次に、ステップS12において、録音プログラム113は、利用条件管理プログラム140に、HDD21に格納されている期限データベース（図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図8のフローチャートに示されている。

ステップS31において利用条件管理プログラム140は、アダプタ26のCPU32と共働して、期限データベース全体のハッシュ値を計算し、ステップS32において、その計算された値と、前回保存しておいたハッシュ値と比較する。

なお、期限データベースにデータが何ら記録されていないとき、

利用条件管理プログラム140は、ハッシュ値を計算しない。

すなわち、HDD21には、期限データベースが形成されており、この期限データベースには、図9に示すように、HDD21に記録されているコンテンツ（コンテンツ）を管理する管理情報として、過去に記録されたことのあるコンテンツのISRCとコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS38において、アダプタ26のCPU32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA(Secure Hash Algorithm)、MD(Message Digest)5などがある。利用条件管理プログラム140は、ステップS31において、CPU32が実行したのと同様にハッシュ値を計算する。そして、ステップS32において、利用条件管理プログラム140は、CPU32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS31で、いま自分自身が計算したハッシュ値とを比較する。

ステップS33において、利用条件管理プログラム140は、ステップS31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致する

か否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム140は、ステップS34において、例えば、録音プログラム113に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インターフェース17を介してディスプレイ20に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されているコンテンツを再生し、HDD21にコピーする処理が禁止される。

ステップS31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS35に進み、利用条件管理プログラム140は、録音プログラム113に、ステップS11で指定されたコピーするコンテンツとして選択されたコンテンツ（選択されたコンテンツ）のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム140は、録音プログラム113に、そのCDのTOCのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

ステップS36において、利用条件管理プログラム140は、ステップS35で取得したISRC（すなわち、選択されたコンテンツ）が期限データベース（図9）に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD21に記録されていないことになるので、ステップS37に進み、利用条件管理プログラム140は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム140は、この現在の日時として、

CPU 32から転送を受けた、アダプタ26のRTC35が出力する値を利用する。そして、ステップS38において、利用条件管理プログラム140は、その時点における期限データベースのデータを読み出し、アダプタ26のCPU32に転送する。CPU32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

次に、ステップS39において、利用条件管理プログラム140は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS13において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

ステップS36において、選択されたコンテンツのISRCが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、HDD21に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップS40に進み、利用条件管理プログラム140は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ26のRTC35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているので、そのコンテンツを再度コピーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場

合には、HDD 21へのコピーが許容される。そこで、ステップS 41に進み、利用条件管理プログラム140は、期限データベースの日時を、過去の登録日時から現在の日時（RTC 35の出力する日時）に変更させる。そして、ステップS 38に戻り、利用条件管理プログラム140は、再び、期限データベース全体のハッシュ値をCPU 32に計算させ、不揮発性メモリ34に保存させるとともに、ステップS 39において、そのコンテンツに対して未登録のフラグを設定する。

一方、ステップS 40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択されたコンテンツのHDD 21へのコピーが禁止される。そこで、この場合には、ステップS 42に進み、利用条件管理プログラム140は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

ステップS 40の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売又は配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップS 40においては、判定の基準は48時間以上の経過としたが、48時間に限らず、例えば、12時間乃至168時間のいずれかの時間であればよい。

以上のようにして、期限データベースチェック処理により、選択されたコンテンツがHDD 21に登録されているか否かを表すフラグが設定される。

図7に戻り、ステップS 13においてコピー管理プログラム13

3は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップS14に進み、コピー管理プログラム133は、録音プログラム113に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ20に表示させる。これにより、使用者は、そのコンテンツをHDD21にコピーすることができない理由を知ることができる。

ステップS13において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップS15に進み、録音プログラム113は、ドライブ22を制御し、そこに装着されているCDからコンテンツを読み出させる。このコンテンツには、図10に示すように、所定の位置にウォーターマークコードが挿入されている。録音プログラム113は、ステップS16において、コンテンツに含まれているウォーターマークコードを抽出し、そのウォーターマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップS18に進み、録音プログラム113は、録音プログラム113に例えば、「コピーは禁止されています」のようなメッセージをインターフェース17を介してディスプレイ20に表示させ、コピー処理を終了させる。

これに対して、ステップS17において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップS19に進み、録音プログラム113は、コンテンツを、圧縮／伸張プログラム138に、例えば、ATRA C(Adaptive Transform Acoustic Codin

g) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。  
ステップ S 2 0 において、録音プログラム 1 1 3 は、暗号化プログラム 1 3 7 に、予め設定され、メモリ 1 3 に記憶されている暗号鍵を用いて、例えば、D E S (Data Encryption Standard) 方式、F E A L (Fast Encipherment Algorithm) 方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ 2 6 の C P U 3 2 により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 2 6 の C P U 3 2 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

次に、ステップ S 2 1 において、録音プログラム 1 1 3 は、暗号化されたデータを、コンテンツデータベース 1 1 4 に転送し、1 つのファイル (コンテンツファイル 1 6 1 として) としてファイル名を付けて H D D 2 1 に保存させる。あるいはまた、1 つのファイルの一部として、そのファイル名の位置情報 (例えば、先頭からのバイト数) を与えて保存するようにしてもよい。

この保存処理と、上記した圧縮符号化処理及び暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

さらに、ステップ S 2 2 において、録音プログラム 1 1 3 は、暗号化プログラム 1 3 7 に、予め定められている不揮発性メモリ 3 4 に記憶されている保存用鍵を使って、上述した D E S 方式、F E A L 方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、



HDD 21の曲データベース（図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する）に保存する。

ステップS23において、録音プログラム113は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者がGUIを介して入力した曲名の情報の要素を組にしてHDD 21の曲データベースに登録する（利用条件ファイル162-1乃至162-Nとして記録する）。そして、ステップS24において、録音プログラム113は、CPU 32に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。

このようにして、例えば、図11に示すような曲データベースが、HDD 21上に登録される。この例においては、アイテム1乃至アイテム3のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ及びコピー条件（SCMS）が記録されている。

例えば、SDMI (Secure Digital Music Initiative) が規定する方式では、CDからコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、3回に設定される。

CDからHDD 21にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ1が故障して、HDD 21に記録されてい

たコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD 21に記録することができる。

また、例えば、ネットワーク2を介してHDD 21に記録されている期限データベースの内容を共有することもできる。

以上においては、I S R Cに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやCDを識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組合せなど）を利用することもできる。

次に、図12乃至図14のフローチャートを参照して、表示操作指示プログラム112及びコンテンツ管理プログラム111を実行するCPU 11及びメインプログラムを実行するCPU 52による、HDD 21からポータブルデバイス6のフラッシュメモリ61（例えば、メモリースティック（商標））に、コンテンツを移動する処理及びチェックアウトの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップS51において、移動管理プログラム134は、利用条件管理プログラム140に、曲データベース全体のハッシュ値を計算させ、ステップS52で、前回CPU 32に計算させ、不揮発性メモリ34に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム134は、ステップS53に進み、表示操作指示プログラム112に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ20に表示させた後、処理を終了させる。この場合の処理は、図8のステップS31乃至ステップS34の処理と同様の処理である。この場合において

は、HDD 21からポータブルデバイス6へのコンテンツの移動が実行されないことになる。

次に、ステップS54において、移動管理プログラム134は、HDD 21に形成されている曲データベース（コンテンツデータベース114に含まれる）から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム112に、選択のためのGUIとしてディスプレイ20に表示させる。使用者は、この選択のためのGUIに基づいて、HDD 21からポータブルデバイス6へ移動させるコンテンツを、図5のフィールド212に表示される曲名、ボタン216などをクリックして選択する。次に、ステップS55において、移動管理プログラム134は、ステップS54で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図15のフローチャートを参照して後述する。

次に、ステップS56において、パーソナルコンピュータ1の認証プログラム141とポータブルデバイス6のCPU53との間において、相互認証処理が行われ、通信用鍵が共有される。

例えば、ポータブルデバイス6のフラッシュメモリ61（又は、EEPROM68）には、マスター鍵KMが予め記憶されており、パーソナルコンピュータ1のRAM13（又は、HDD 21の所定のファイル）には、個別鍵KPとIDが予め記憶されているものとする。CPU53は、認証プログラム141から、RAM13に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMにハッシュ関数を適用して、RAM13に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。

このようにすることで、パーソナルコンピュータ 1 とポータブルデバイス 6 の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

あるいはまた、パーソナルコンピュータ 1 の RAM 13 に ID とマスター鍵 KMP を予め記憶させておくとともに、ポータブルデバイス 6 のフラッシュメモリ 61 にもポータブルデバイス 6 の ID とマスター鍵 KMM を記憶させておく。そして、それぞれの ID とマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきた ID とマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9798-2 を利用することができる。

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップ S 57 において、移動管理プログラム 134 は、コンテンツデータベース 114 に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図 7 のステップ S 20 の処理で暗号化されている）を HDD 21 から読み出す。ステップ S 58 において、移動管理プログラム 134 は、ステップ S 57 で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップ S 19 の処理）、暗号化方式（ステップ S 20 の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス 6 のものに変換する処理を実行する。この変換処理の詳細は、図 17 のフロ

ーチャートを参照して後述する。

ステップS 5 9において、移動管理プログラム1 3 4は、PD用ドライバ1 4 3に、ステップS 5 8で変換したコンテンツを、USBポート2 3を介してポータブルデバイス6に転送させる。ステップS 6 0において、ポータブルデバイス6のCPU 5 3は、USBコネクタ5 6を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ6 1に記憶させる。

ステップS 6 1において、移動管理プログラム1 3 4は、さらに、利用条件変換プログラム1 3 9に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス6が管理している形式に変換する。ステップS 6 2において、移動管理プログラム1 3 4は、さらに、利用条件変換プログラム1 3 9に、選択されたコンテンツの曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス6の管理する形式に変換させる。そして、ステップS 6 3において、移動管理プログラム1 3 4は、PD用ドライバ1 4 3に、ステップS 6 1で変換した再生条件と、ステップS 6 2で変換したSCMS情報を、ポータブルデバイス6に転送させる。ポータブルデバイス6のCPU 5 3は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ6 1に保存する。

ステップS 6 4において、移動管理プログラム1 3 4はまた、PD用ドライバ1 4 3に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU 1 1が曲データベース中で扱っている形式のまま、ポータブルデバイス6に転送させ、フラッシュメモリ6 1に保存させる。

ステップS 6 5において、移動管理プログラム1 3 4は、コンテンツデータベース1 1 4に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップS 6 6において、復号プログラム1 4 2に、その暗号鍵をR A M 1 3に保存されている保存用鍵で復号させ、暗号化プログラム1 3 7に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム1 3 4は、P D用ドライバ1 4 3に、ポータブルデバイス6へ転送させる。

ポータブルデバイス6のC P U 5 3は、ステップS 6 7で、パーソナルコンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ6 1に保存する。

C P U 5 3は、暗号鍵の保存が完了すると、ステップS 6 8において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1の移動管理プログラム1 3 4は、ポータブルデバイス6からこの通知を受けると、ステップS 6 9において、コンテンツデータベース1 1 4に、そのコンテンツに対応するコンテンツファイル1 6 1を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル1 6 2）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS 7 0において、移動管理プログラム1 3 4は、アダプタ2 6のC P U 3 2に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ3 4に保存させる。このハッシュ値が、上

述したステップS 5 2において、前回保存しておいたハッシュ値として用いられることになる。

次に、パーソナルコンピュータ 1 からポータブルデバイス 6 にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ 1 からポータブルデバイス 6 にコンテンツをチェックアウトする処理は、図 1 2 乃至図 1 4 のパーソナルコンピュータ 1 からポータブルデバイス 6 へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ 1 においてチェックイン／チェックアウト管理プログラム 1 3 2 により実行され、図 1 4 のステップS 6 9において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（又はチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

次に、コンテンツ管理プログラム 1 1 1 を実行するCPU 1 1 による、図 1 2 のステップS 5 5 における選択されたコンテンツの再生条件などのチェック処理について図 1 5 のフローチャートを参照して説明する。ステップS 8 1 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、曲データベースから、各種の条件を読み出させる。移動管理プログラム 1 3 4 は、ステップS 8 2 において、ステップS 8 1 で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既に過ぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS 8 3 に進み、移

動管理プログラム 134 は、表示操作指示プログラム 112 に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ 20 に表示させ、処理を終了させる。ステップ S82 において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップ S84 に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ 26 の RTC 35 より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ 1 の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム 134 は、この現在日時を CPU 32 から提供を受けて、ステップ S84 の判断を自ら行うか、又は、ステップ S81 で、曲データベースから読み出した再生条件をアダプタ 26 の CPU 32 に供給し、CPU 32 に、ステップ S84 の判定処理を実行させる。

現在日時が再生終了日時を過ぎている場合、ステップ S85 に進み、移動管理プログラム 134 は、コンテンツデータベース 114 に、選択されたコンテンツを HDD 21 から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップ S86 において、移動管理プログラム 134 は、CPU 32 に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ 34 に保存させる。以後、処理は終了される。したがって、この場合、コンテンツの移動が実行されない。

ステップ S84 において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップ S87 に進み、移動管理プログラム 134 は、その選択されたコンテンツの再生時課金条件（例えば、



再生1回当たりの料金)が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム134は、ステップS88において、PD用ドライバ143に、ポータブルデバイス6と通信させ、ポータブルデバイス6に課金機能が存在するか否かを判定する。ポータブルデバイス6に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス6に転送する訳にはいかないので、ステップS89において、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ20に表示させ、コンテンツの移動処理を終了させる。

ステップS87において再生時課金条件が登録されていないと判定された場合、又は、ステップS88において、ポータブルデバイス6に課金機能が存在すると判定された場合、ステップS90に進み、移動管理プログラム134は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS91に進み、移動管理プログラム134は、ポータブルデバイス6に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス6が、その再生条件を守る機能を有していない場合には、ステップS92に進み、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ20に表示させ、処理を終了させる。

ステップS90において、再生条件が登録されていないと判定さ

れた場合、又はステップS 9 1において、ポータブルデバイス 6 が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図 1 2 のステップ S 5 6 に戻る。

図 1 6 は、ポータブルデバイス 6 が管理している（守ることが可能な）再生条件の例を表している。図 1 6 に示す再生情報は、例えば、E E P R O M 6 8 に記憶されている。この例においては、アイテム 1 乃至アイテム 3 の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム 2 についてのみ登録されており、アイテム 1 とアイテム 3 については登録されていない。したがって、アイテム 2 のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム 1 又はアイテム 3 のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

次に、図 1 7 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する C P U 1 1 による、図 1 2 のステップ S 5 8 におけるフォーマット変換処理の詳細について説明する。ステップ S 1 0 1 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップ S 1 0 2 において、移動管理プログラム 1 3 4 は、相手先の機器（今の場合、ポータブルデバイス 6）に設定することが可能な条件を調べる。すなわち、移動管理プログラム 1 3 4 は、ポータブルデバイス 6 の C P U 5 3 に設定可能な条件を問い合わせ、その回答を得る。ステップ S 1 0 3 において移動管理プログラム 1 3 4 は、曲データベース中に登録されている

フォーマットの条件のうち、相手先の機器に設定可能な条件をステップS 1 0 2で調べた条件に基づいて決定する。

ステップS 1 0 4において、移動管理プログラム 1 3 4は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS 1 0 5に進み、コンテンツをポータブルデバイス 6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス 6が守ることができないので、そのようなポータブルデバイス 6には、コンテンツを移動することが禁止されるのである。

ステップS 1 0 4において設定可能な条件が存在すると判定された場合、ステップS 1 0 6に進み、移動管理プログラム 1 3 4は、利用条件変換プログラム 1 3 9に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス 6に転送する際、ヘッドに格納される条件）に変換させる。そして、ステップS 1 0 7において、移動管理プログラム 1 3 4は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス 6は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

次に、図 1 8乃至図 2 0のフローチャートを参照して、コンテンツ管理プログラム 1 1 1を実行するCPU 1 1及びメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス 6にコンテンツをコピーする場合の処理について説明する。この図 1 8乃至図 2 0のステップS 1 1 1乃至ステップS 1 2 7の処理は、コピー管理プログラム 1 3 3により実行され、図 1 2乃至図 1 4のHDD 2 1からポータブルデバイス 6へコンテンツを移動させ

る場合のステップS 5 1乃至ステップS 6 7の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス6と、パーソナルコンピュータ1との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ1のHDD 2 1からポータブルデバイス6のフラッシュメモリ 6 1に転送され、保存される。その後、ステップS 1 2 8において、コピー管理プログラム1 3 3は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS 1 2 9において、コピー管理プログラム1 3 3は、CPU 3 2に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ 3 4に保存させる。

次に、図2 1のフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1及びメインプログラムを実行するCPU 5 3による、ポータブルデバイス6からHDD 2 1にコンテンツを移動する処理及びチェックインの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップS 1 6 1において、移動管理プログラム1 3 4は、ポータブルデバイス6のCPU 5 3に対してフラッシュメモリ 6 1に記憶されているコンテンツの情報の読み出しを要求する。CPU 5 3は、この要求に対応して、フラッシュメモリ 6 1に記憶されているコンテンツの情報をパーソナルコンピュータ1に送信する。移動管理プログラム1 3 4は、この情報に基づいて、ディスプレイ2 0に、フラッシュメモリ 6 1に記憶されているコンテンツを選択するためのGUIを表示させる。使用者は、キーボード1 8又はマウス1 9を操作して、

そのGUIに基づいて、ポータブルデバイス6からHDD21（コンテンツデータベース114）に移動させるコンテンツを指定する。

ステップS162において、移動管理プログラム134は、認証プログラム141に、CPU53との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図12のステップS56における場合と同様の処理である。

次に、ステップS163において、CPU53は、フラッシュメモリ61に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ1に転送する。移動管理プログラム134は、ステップS164において、ポータブルデバイス6から転送されてきたコンテンツを、1つのファイルとしてファイル名を付けて、コンテンツデータベース114（HDD21）に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

ステップS165において、CPU53は、フラッシュメモリ61に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図14のステップS67の処理でフラッシュメモリ61に保存されていたものである。

ステップS166において、移動管理プログラム134は、ポータブルデバイス6から暗号鍵の転送を受けると、復号プログラム142に、それを通信用鍵で復号させ、暗号化プログラム137に、自分自身の保存用鍵で暗号化させる。ステップS167で、移動管

理プログラム 134 は、コンテンツデータベース 114 に、ステップ S164 で保存したコンテンツのファイル名、そのコンテンツの情報、使用者が GUI を介して入力した曲名、ステップ S166 で暗号化した暗号鍵などを、HDD 21 の曲データベースに登録させる。そして、ステップ S168 において、移動管理プログラム 134 は、利用条件管理プログラム 140 に、その曲データベース全体のハッシュ値を CPU 32 に計算させ、不揮発性メモリ 34 に保存させる。

ステップ S169 において、移動管理プログラム 134 は、ポータブルデバイス 6 に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU 53 は、パーソナルコンピュータ 1 から、そのコンテンツの削除が要求されてきたとき、ステップ S170 において、フラッシュメモリ 61 に記憶されているそのコンテンツを削除する。

次に、ポータブルデバイス 6 からパーソナルコンピュータ 1 にコンテンツをチェックインする処理について説明する。ポータブルデバイス 6 からパーソナルコンピュータ 1 にコンテンツをチェックインする処理は、図 21 のポータブルデバイス 6 からパーソナルコンピュータ 1 へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ 1 においてチェックイン/チェックアウト管理プログラム 132 により実行され、図 21 のステップ S162 乃至 S166 の処理が省略される。また、パーソナルコンピュータ 1 は、図 21 のステップ S167 において、曲データベースに登録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、

ステップS 1 7 0の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

なお、ポータブルデバイス6のフラッシュメモリ61がメモリカードとして着脱可能であるとき、パーソナルコンピュータ1は、チェックインの処理において、図21のステップS 1 6 2の相互認証の処理を実行する。

次に、コンテンツ管理プログラム111を実行するCPU11及びメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21へコンテンツをコピーする場合の処理について、図22のフローチャートを参照して説明する。この図22に示すステップS 1 8 1乃至ステップS 1 8 8の処理は、図21のポータブルデバイス6からHDD21へコンテンツを移動させる場合の処理におけるステップS 1 6 1乃至ステップS 1 6 8の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム133により実行され、図21のステップS 1 6 9, S 1 7 0の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

次に、図23のフローチャートを参照して、EMDサーバ4及びコンテンツ管理プログラム111を実行するCPU11による、EMDサーバ4から転送を受けたコンテンツをHDD21にコピーする処理について説明する。ステップS 2 0 1において、購入用プログラム144は、図5に示すボタン202がクリックされて、使用者からEMDサーバ4へのアクセスが指令されたとき、通信部25を制御し、ネットワーク2を介してEMDサーバ4にアクセスさせ

る。E M Dサーバ4は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク2を介してパーソナルコンピュータ1に転送する。購入用プログラム144は、通信部25を介して、この情報を取得したとき、表示操作指示プログラム112に、それをインターフェース17を介してディスプレイ20に表示させる。使用者は、ディスプレイ20に表示されたG U Iを利用して、ステップS 202において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク2を介してE M Dサーバ4に転送される。ステップS 203において、購入用プログラム144は、E M Dサーバ4との間において、ネットワーク2を介して相互認証処理を実行し、通信用鍵を共有する。

パーソナルコンピュータ1とE M Dサーバ4との間で行われる相互認証処理は、例えば、I S O 9798-3で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ1は、自分自身の秘密鍵とE M Dサーバ4の公開鍵を予め有しており、E M Dサーバ4は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ1の公開鍵は、E M Dサーバ4から転送したり、あるいはパーソナルコンピュータ1に予め配布されている証明書(certificate)をパーソナルコンピュータ1からE M Dサーバ4に転送し、その証明書をE M Dサーバ4が確認し、公開鍵を得るようにしてもよい。さらに、ステップS 204において、購入用プログラム144は、E M Dサーバ4との間において課金に関する処理を実行する。この課金の処理の詳細は、図24のフローチャートを参照して後述する。



次に、ステップS 2 0 5において、EMDサーバ4は、パーソナルコンピュータ1に対して、ステップS 2 0 2で指定された、暗号化されているコンテンツをネットワーク2を介してパーソナルコンピュータ1に転送する。このとき、時刻情報も適宜転送される。ステップS 2 0 6において、購入用プログラム1 4 4は、コンテンツデータベース1 1 4に、転送を受けたコンテンツにファイル名を付けてHDD 2 1に1つのコンテンツファイル1 6 1として保存させる。ステップS 2 0 7において、EMDサーバ4は、さらに、そのコンテンツの暗号鍵をステップS 2 0 3でパーソナルコンピュータ1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ1へ転送する。

購入用プログラム1 4 4は、ステップS 2 0 8において、復号プログラム1 4 2に、EMDサーバ4より転送を受けた暗号鍵を単独で、又はアダプタ2 6のCPU 3 2と共同して通信用鍵を用いて復号させ、暗号化プログラム1 3 7に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップS 2 0 9において、購入用プログラム1 4 4は、コンテンツデータベース1 1 4に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD 2 1の曲データベースに登録させる。さらに、ステップS 2 1 0において、購入用プログラム1 4 4は、その曲データベース全体のハッシュ値をCPU 3 2に計算させ、不揮発性メモリ3 4に保存させる。

なお、ステップS 2 0 5においてEMDサーバ4は、コンテンツとともに、時刻データをパーソナルコンピュータ1に送信する。この時刻データは、パーソナルコンピュータ1からアダプタ2 6に転

送される。アダプタ 26 の CPU 32 は、パーソナルコンピュータ 1 より転送されてきた時刻データを受信すると、ステップ S 211 において、RTC 35 の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ 26 の RTC 35 の時刻情報を修正するようにしたので、アダプタ 26 を常に正しい時刻情報を保持することが可能となる。

次に、図 24 のフローチャートを参照して、EMD サーバ 4 及びコンテンツ管理プログラム 111 を実行する CPU 11 による、図 23 のステップ S 204 における課金に関する処理の詳細について説明する。ステップ S 221 において、購入用プログラム 144 は、ステップ S 201 で EMD サーバ 4 から伝送されてきた価格情報の中から、ステップ S 202 で指定された選択されたコンテンツの価格情報を読み取り、これを HDD 21 上の課金ログに書き込む。図 25 は、このような課金ログの例を表している。この例においては、使用者は、アイテム 1 乃至アイテム 3 を、EMD サーバ 4 からコピーしており、アイテム 1 とアイテム 2 の領域は 50 円とされ、アイテム 3 の料金は 60 円とされている。その時点における課金ログのハッシュ値も、CPU 32 により計算され、不揮発性メモリ 34 に登録されている。

次に、ステップ S 222 において、購入用プログラム 144 は、ステップ S 221 で書き込んだ課金ログを HDD 21 から読み出し、これをネットワーク 2 を介して EMD サーバ 4 に転送する。EMD サーバ 4 は、ステップ S 223 において、パーソナルコンピュータ 1 から転送を受けた課金ログに基づく課金計算処理を実行する。す

なわち、EMDサーバ4は、内蔵するデータベースに、パーソナルコンピュータ1の使用者から伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ4は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ4は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

次に、図26と図27のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、音声入出力インターフェース24のIEC60958端子24aから入力された、図示せぬCDプレーヤなどからの再生されたコンテンツを、HDD21にコピーする場合の処理について説明する。ステップS241において、使用者は、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インターフェース24のIEC60958端子24aに接続する。ステップS242において、使用者は、キーボード18又はマウス19を操作し、CDプレーヤからコピーするコンテンツの曲名（又は、コンテンツに対応する番号）を入力する。そして、ステップS243において使用者は、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1のキ

ーボード 18 又はマウス 19 を介して再生開始指令を入力することで、CD プレーヤに CD の再生を開始させることも可能である。

CD プレーヤにおいて、CD の再生が開始されると、ステップ S 244 において、CD プレーヤから出力されたコンテンツが、IEC 60958 端子 24a を介してパーソナルコンピュータ 1 に転送されてくる。ステップ S 245 において、コピー管理プログラム 133 は、IEC 60958 端子 24a を介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。この SCMS データには、コピー禁止、コピー 1 回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップ S 246 において、CPU 11 は、SCMS データがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップ S 247 に進み、コピー管理プログラム 133 は、表示操作指示プログラム 112 に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ 20 に表示させ、コピー処理を終了する。すなわち、この場合には、HDD 21 へのコピーが禁止される。

コピー管理プログラム 133 は、ステップ S 246 において、ステップ S 245 で読み取った SCMS 情報がコピー禁止を表していないと判定した場合、ステップ S 248 に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップ S 249 において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップ S 247 に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

ステップS 2 4 9において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップS 2 5 0に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップS 2 5 1, S 2 5 2の処理で、処理が終了される。この処理は、図7のステップS 1 3, S 1 4の処理と同様の処理である。

選択されたコンテンツがまだHDD 2 1に登録されていないコンテンツであれば、ステップS 2 5 3乃至S 2 5 8で、その登録処理が実行される。このステップS 2 5 3乃至ステップS 2 5 8の処理は、ステップS 2 5 7において、IEC 6 0 9 5 8端子2 4 aから供給されてくるSCMS情報も曲データベースに登録される点を除き、図7のステップS 1 9乃至ステップS 2 4の処理と同様の処理であるので、その説明は省略する。

次に、図28と図29のフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1による、コンテンツをHDD 2 1からIEC 6 0 9 5 8端子2 4 aに出力（再生）する場合の処理について説明する。ステップS 2 7 1乃至ステップS 2 7 3において、図18のステップS 1 1 1乃至S 1 1 3における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS 2 7 4に進み、表示操作指示プログラム1 1 2は、コンテンツ管理プログラム1 1 1を介して、コンテンツデータベース1 1 4に、HDD 2 1の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、

ディスプレイ 20 に表示させる。使用者は、その表示を見て、キーボード 18 又はマウス 19 を適宜操作して、再生出力するコンテンツを選択する。ステップ S 275 において、表示操作指示プログラム 112 は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図 30 のフローチャートを参照して後述する。

次に、ステップ S 276 において、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、ステップ S 274 において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム 142 に保存用鍵で復号させる。ステップ S 277 において、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、選択されたコンテンツの S CMS 情報を曲データベースから読み出させ、IEC 60958 端子 24a から出力する S CMS 情報を、S CMS システムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は 1 だけインクリメントされ、新たな S CMS 情報とされる。ステップ S 278 において、表示操作指示プログラム 112 はさらに、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、選択されたコンテンツの I SRC を曲データベースから読み出させる。

次に、ステップ S 279 において、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツを H

DD 2 1 から読み出させる。表示操作指示プログラム 1 1 2 はさらに、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム 1 4 2 に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム 1 3 8 は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップ S 2 8 0 において、表示操作指示プログラム 1 1 2 は、ドライバ 1 1 7 に、ステップ S 2 7 9 で、復号したデジタルデータであるコンテンツを、ステップ S 2 7 7 で決定した SCMS 情報、並びにステップ S 2 7 8 で読み出した ISRC 情報とともに、IEC 6 0 9 5 8 の規定に従って、IEC 6 0 9 5 8 端子 2 4 a から出力させる。さらにまた、表示操作指示プログラム 1 1 2 は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インターフェース 2 4 のアナログ出力端子から出力させる。

ステップ S 2 8 1 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、曲データベース中の再生回数カウンタの値を 1 だけインクリメントさせる。そして、ステップ S 2 8 2 において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップ S 2 8 3 に進み、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、対応する料金を課金ログに書き込ませ、ステップ S 2 8 4 において、表示操

作指示プログラム 112 は、利用条件管理プログラム 140 に、曲データベース全体のハッシュ値を CPU 32 に計算させ、不揮発性メモリ 34 に記憶させる。ステップ S 282 において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップ S 283 とステップ S 284 の処理はスキップされる。

次に、図 30 のフローチャートを参照して、コンテンツ管理プログラム 111 を実行する CPU 11 による、図 28 のステップ S 275 の再生条件等のチェック処理の詳細について説明する。ステップ S 301 において、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、曲データベースの各種条件を読み出させる。ステップ S 302 において利用条件管理プログラム 140 は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップ S 303 に進み、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、選択されたコンテンツを HDD 21 から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップ S 304 において、表示操作指示プログラム 112 はさらに、利用条件管理プログラム 140 に、曲データベースの新たなハッシュ値を CPU 32 に計算させ、そのハッシュ値を不揮発性メモリ 34 に保存させる。この場合、再生出力は禁止される。

ステップ S 302 において、再生回数が制限回数を過ぎていないと判定された場合、ステップ S 305 に進み、利用条件管理プログラム 140 2 は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した



場合と同様にステップS 3 0 3において、選択されたコンテンツをHDD 2 1から削除させるとともに、曲データベースからも削除させる。そして、ステップS 3 0 4において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

ステップS 3 0 5において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップS 3 0 6に進み、CPU 3 2は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS 3 0 7に進み、表示操作指示プログラム1 1 2は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ2 0に表示させる。ステップS 3 0 6において、再生時課金条件が付加されていないと判定された場合、ステップS 3 0 7の処理はスキップされる。

次に、図3 1と図3 2のフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1及びメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス6経由でコンテンツを出力（再生）する場合の処理について説明する。ステップS 3 2 1乃至ステップS 3 2 5において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図2 8のステップS 2 7 1乃至ステップS 2 7 5の処理と同様の処理であるので、その説明は省略する。

ステップS 3 2 6において、ポータブルデバイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信

用鍵が共有される。ステップS 3 2 7において、表示操作指示プログラム1 1 2は、ポータブルデバイス6に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップS 3 2 8において、表示操作指示プログラム1 1 2は、ステップS 3 2 4で、コンテンツ管理プログラム1 1 1を介してコンテンツデータベース1 1 4に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD 2 1から読み出させる。表示操作指示プログラム1 1 2は、ステップS 3 2 9において、コンテンツ管理プログラム1 1 1に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス6の方式のものに変換する処理を実行させる。そして、ステップS 3 3 0において、表示操作指示プログラム1 1 2は、暗号化プログラム1 3 7に、ステップS 3 2 9において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス6に転送する。

ステップS 3 3 1において、ポータブルデバイス6のCPU 5 3は、ステップS 3 2 7において、パーソナルコンピュータ1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS 3 3 2において、表示操作指示プログラム1 1 2は、コンテンツ管理プログラム1 1 1を介してコンテンツデータベース1 1 4に、曲データベースの再生回数カウンタを1だけインクリメントさせる。さらに、ステップS 3 3 3において、表示操作指示プログラム1 1 2は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS 3 3 4において、コンテンツ管理プログラム

1 1 1 を介してコンテンツデータベース 1 1 4 に、その料金を課金ログに書き込ませ、ステップ S 3 3 5 において、CPU 3 2 に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップ S 3 3 4，ステップ S 3 3 5 の処理はスキップされる。

本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU 1 1 を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

さらに、上述したように、CPU 1 1 の機能の一部は、ハードウェアとしてのアダプタ 2 6 に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ 2 6 の不揮発性メモリ 3 4 に保存される。すなわち、図 8 のステップ S 3 2，S 3 3 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 3 4 に記憶されているものとされる。これにより、例えば、他の記録媒体にコピー又は移動させる前に、HDD 2 1 に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD 2 1 から、そこに保存されているコンテンツを他の記録媒体にコピー又は移動した後、HDD 2 1 にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピー又は移動ができてしまうようなこと

が防止される。

例えば、図 3 3 に示すように、HDD 2 1 にコンテンツ A, B が保存されている場合、不揮発性メモリ 3 4 には、コンテンツ A とコンテンツ B の情報に対応するハッシュ値が保存されている。この状態において、HDD 2 1 のコンテンツ A, B を含む記録データの一部又は全部を他の記録媒体 2 7 1 にバックアップしたとする。その後、HDD 2 1 に保存されているコンテンツ A とコンテンツ B のうち、コンテンツ A を他の記録媒体 2 7 2 に移動させた場合、その時点において、HDD 2 1 に記録されているコンテンツは、コンテンツ B だけとなるので、不揮発性メモリ 3 4 のハッシュ値も、コンテンツ B に対応するハッシュ値に変更される。

したがって、その後、記録媒体 2 7 1 にバックアップしておいた HDD 2 1 のコンテンツ A, B を含む記録データの一部又は全部を HDD 2 1 にリストアして、HDD 2 1 に、再びコンテンツ A とコンテンツ B を保存させたとしても、不揮発性メモリ 3 4 には、コンテンツ B の情報から演算されたハッシュ値が記憶されており、コンテンツ A とコンテンツ B の情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 2 1 に記憶されているコンテンツ A とコンテンツ B に基づくハッシュ値が、不揮発性メモリ 3 4 に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 2 1 に保存されているコンテンツ A とコンテンツ B の利用が制限されてしまうことになる。

さらに、上述したように、アダプタ 2 6 は、RTC 3 5 を内蔵しており、この RTC 3 5 の値は、正しい認証結果が得られた他の装

置（例えば、E M Dサーバ４）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ１が管理するものではなく、R T C 3 5が出力するものが利用される。したがって、使用者が、パーソナルコンピュータ１の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

また、アダプタ２６は、暗号化されて転送されてきたプログラムをR O M 3 6に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図３４のフローチャートを参照して説明する。

すなわち、パーソナルコンピュータ１は、アダプタ２６に対して、所定の処理を実行させたいとき、ステップS 3 5 1において、アダプタ２６に実行させるべきプログラムをR A M 1 3に予め記憶されている暗号鍵を用いて暗号化してアダプタ２６に転送する。アダプタ２６のR O M 3 6には、パーソナルコンピュータ１から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。C P U 3 2は、このR O M 3 6に記憶されているプログラムに従って、パーソナルコンピュータ１から転送されてきた暗号化されているプログラムをステップS 3 5 2において復号する。そして、ステップS 3 1 3において、C P U 3 2は、復号したプログラムをR A M 3 3に展開し、ステップS 3 5 4において、そのプログラムを実行する。

例えば、上述したように、パーソナルコンピュータ１のC P U 1 1は、H D D 2 1の曲データベースのハッシュ値をアダプタ２６に計算させるとき、曲データベースのデータを暗号鍵で暗号化してア

アダプタ 26 の CPU 32 に転送する。CPU 32 は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ 34 に記憶させる。あるいは、そのハッシュ値を、CPU 32 は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ 1 の CPU 11 に転送する。

図 35 は、アダプタ 26 の内部のより具体的な構成を表している。アダプタ 26 は、半導体 IC として形成される。アダプタ 26 は、図 2 に示したインターフェース 31、CPU 32、RAM 33、不揮発性メモリ 34、RTC 35、ROM 36 以外に、RAM 33 に対する書き込みと読み出しを制御する RAM コントローラ 301、並びに論理回路 302 を有している。論理回路 302 は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ 26 から直接出力するような場合の処理のために用いられる。

これらのインターフェース 31 乃至 ROM 36、RAM コントローラ 301 並びに論理回路 302 は、半導体 IC 内に一体的に組み込まれ、外部からは分解できないように構成されている。

水晶振動子 311 は、アダプタ 26 が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路 312 は、RTC 35 を動作させるための発振回路である。バッテリー 313 は、発振回路 312、不揮発性メモリ 34 及び RTC 35 に対してバックアップ用の電力を供給している。アダプタ 26 のその他の回路には、パーソナルコンピュータ 1 の電源供給回路 321 からの電力が供給されている。

不揮発性メモリ 34 は、書き込み消去可能な ROM で構成するこ

とも可能であるが、バッテリー 313 からのバックアップ電源でバックアップされる RAM で構成する場合には、例えば、図 36A 及び図 36B に示すように、不揮発性メモリ 34 の上に保護アルミニウム層 351 を形成し、さらに、その保護アルミニウム層 351 と同一平面上となるように、不揮発性メモリ 34 にバッテリー 313 からの電力を供給する電源パターン 352 を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ 34 を改竄すべく、保護アルミニウム層 351 を削除しようとする、同一平面上の電源パターン 352 も削除されてしまい、不揮発性メモリ 34 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

さらに、図 37 に示すように、不揮発性メモリ 34 に対するデータの書き込み又は読み出しのための配線 401-1 乃至 401-3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 401-3 からデータを読み出すためには、上方の配線 401-1, 401-2 を除去しなければならず、複数の配線 401-1, 401-2, 401-3 から同時にデータを読み取ることができなくなる。

さらにまた、不揮発性メモリ 34 は、配線 401-1 乃至 401-3 を冗長に形成するようにすることができる。例えば、不揮発性メモリ 34 内部に形成される配線 401-1 乃至 401-3 が不揮発性メモリ 34 を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにするこ

とで、配線 401-1 乃至 401-3 の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

不揮発性メモリ 34 からデータを読み出すために設計されている専用の回路（半導体 IC としてのアダプタ 26 に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ 34 が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ 34 に記憶されているデータを読み出すべく、プローブを配線 401-1 乃至 401-3 に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

次に、ポータブルデバイス 6 がパーソナルコンピュータ 1 から所定のデータを受け取る場合の、相互認証の処理を図 38 及び図 39 のフローチャートを参照して説明する。ステップ S401 において、パーソナルコンピュータ 1 の CPU 11 は、乱数 N<sub>a</sub> を生成する。ステップ S402 において、パーソナルコンピュータ 1 の CPU 11 は、インターフェース 17 に、パーソナルコンピュータ 1 の ID、鍵のカテゴリ番号 G 及び乱数 N<sub>a</sub> をポータブルデバイス 6 へ送信させる。

ステップ S421 において、ポータブルデバイス 6 の CPU 53 は、乱数 N<sub>b</sub> を生成する。ステップ S422 において、ポータブルデバイス 6 は、パーソナルコンピュータ 1 からインターフェース 17 を介して送信されたパーソナルコンピュータ 1 の ID、鍵のカテゴリ番号 G 及び乱数 N<sub>a</sub> を受信する。ステップ S423 において、ポータブルデバイス 6 の CPU 53 は、鍵のカテゴリ番号 G から、



マスター鍵  $KMa$  の鍵番号  $j$  を求める。

ステップ  $S424$  において、ポータブルデバイス 6 の CPU 53 は、 $j$  番目のマスター鍵  $KMa[j]$  を求める。ステップ  $S425$  において、ポータブルデバイス 6 の CPU 53 は、パーソナルコンピュータ 1 の ID に、マスター鍵  $KMa[j]$  を基にした SHA などのハッシュ関数を適用し、鍵  $Kab$  を求める。

ステップ  $S426$  において、ポータブルデバイス 6 の CPU 53 は、乱数  $Na$ 、乱数  $Nb$  及びパーソナルコンピュータ 1 の ID に、鍵  $Kab$  を基にした SHA などのハッシュ関数を適用し、乱数  $R1$  を求める。ステップ  $S427$  において、ポータブルデバイス 6 の CPU 53 は、乱数  $Sb$  を生成する。

ステップ  $S428$  において、ポータブルデバイス 6 の CPU 53 は、USB コントローラ 57 に、乱数  $Na$ 、乱数  $Nb$ 、鍵番号  $j$  及び乱数  $Sb$  をパーソナルコンピュータ 1 へ送信させる。

ステップ  $S403$  において、パーソナルコンピュータ 1 は、インターフェース 17 を介して、乱数  $Na$ 、乱数  $Nb$ 、鍵番号  $j$  及び乱数  $Sb$  を受信する。ステップ  $S404$  において、パーソナルコンピュータ 1 の CPU 11 は、鍵番号  $j$  を基に、個別鍵  $KIa$  に含まれる鍵  $Kab$  を求める。ステップ  $S405$  において、パーソナルコンピュータ 1 の CPU 11 は、乱数  $Na$ 、乱数  $Nb$  及びパーソナルコンピュータ 1 の ID に、鍵  $Kab$  を基にした SHA などのハッシュ関数を適用し、乱数  $R2$  を求める。

ステップ  $S406$  において、パーソナルコンピュータ 1 の CPU 11 は、受信した乱数  $R1$  と、ステップ  $S405$  で生成した乱数  $R2$  とが等しいか否かを判定し、乱数  $R1$  と乱数  $R2$  とが等しくない

と判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス 6 を認証せず、処理は終了する。ステップ S 4 0 6 において、乱数 R 1 と乱数 R 2 とが等しいと判定された場合、ポータブルデバイス 6 は正当なポータブルデバイスなので、ステップ S 4 0 7 に進み、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 S a を生成する。

ステップ S 4 0 8 において、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 N b 及び乱数 N a に、鍵 K a b を基にした S H A などのハッシュ関数を適用し、乱数 R 3 を求める。ステップ S 4 0 9 において、パーソナルコンピュータ 1 の CPU 1 1 は、インターフェース 1 7 に、乱数 R 3 及び乱数 S b をポータブルデバイス 6 へ送信させる。ステップ S 4 1 0 において、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 S a 及び乱数 S b に、鍵 K a b を基にした S H A などのハッシュ関数を適用し、一時鍵 K s を求める。

ステップ S 4 2 9 において、ポータブルデバイス 6 の CPU 5 3 は、乱数 R 3 及び乱数 S b を受信する。ステップ S 4 3 0 において、ポータブルデバイス 6 の CPU 5 3 は、乱数 N b 及び乱数 N a に、鍵 K a b を基にした S H A などのハッシュ関数を適用し、乱数 R 4 を求める。ステップ S 4 3 1 において、ポータブルデバイス 6 の CPU 5 3 は、受信した乱数 R 3 と、ステップ S 4 3 0 で生成した乱数 R 4 とが等しいか否かを判定し、乱数 R 3 と乱数 R 4 とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ 1 を認証せず、処理は終了する。ステップ S 4 3 1 において、乱数 R 3 と乱数 R 4 とが等しいと判定された場合、パーソナルコンピュータ 1 は正当なパーソナルコンピュー

タなので、ステップS 4 3 2に進み、ポータブルデバイス6のCPU 5 3は、乱数S a及び乱数S bに、鍵K a bを基にしたSHAなどのハッシュ関数を適用し、一時鍵K sを求める。

以上のように、パーソナルコンピュータ1及びポータブルデバイス6は、相互認証し、共通の一時鍵K sを得る。なお、ステップS 4 2 5、ステップS 4 2 6、ステップS 4 0 5、ステップS 4 0 8、ステップS 4 1 0、ステップS 4 3 0及びステップS 4 3 2において、SHAなどのハッシュ関数を適用するとして説明したが、DESなどを適用しても良い。

次に、パーソナルコンピュータ1がポータブルデバイス6に所定のデータを送信する場合の、相互認証の処理を図4 0及び図4 1のフローチャートを参照して説明する。ステップS 4 5 1において、パーソナルコンピュータ1のCPU 1 1は、乱数N aを生成する。ステップS 4 5 2において、パーソナルコンピュータ1は、インターフェース1 7を介して、パーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテゴリ番号G p、ポータブルデバイス6の鍵のカテゴリ番号G s及び乱数N aをポータブルデバイス6に送信する。

ステップS 4 8 1において、ポータブルデバイス6のCPU 5 3は、乱数N bを生成する。ステップS 4 8 2において、ポータブルデバイス6は、パーソナルコンピュータ1からインターフェース1 7を介して送信されたパーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテゴリ番号G p、ポータブルデバイス6の鍵のカテゴリ番号G s及び乱数N aを受信する。ステップS 4 8 3において、ポータブルデバイス6のCPU 5 3は、ポータブルデ

バイス 6 の鍵のカテゴリ番号  $G_s$  から、マスター鍵  $KMa$  の鍵番号  $j$  を求める。

ステップ S 4 8 4 において、ポータブルデバイス 6 の CPU 5 3 は、 $j$  番目のマスター鍵  $KMa[j]$  を求める。ステップ S 4 8 5 において、ポータブルデバイス 6 の CPU 5 3 は、パーソナルコンピュータ 1 の ID に、マスター鍵  $KMa[j]$  を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、鍵  $Kab$  を求める。ステップ S 4 8 6 において、ポータブルデバイス 6 の CPU 5 3 は、パーソナルコンピュータ 1 の鍵のカテゴリ番号  $G_p$  を基に、マスター鍵  $KIa$  の鍵番号  $k$  を求める。ステップ S 4 8 7 において、ポータブルデバイス 6 の CPU 5 3 は、鍵  $Kab$  に、マスター鍵  $KIa[k]$  を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、鍵  $K'ab$  を求める。

ステップ S 4 8 8 において、ポータブルデバイス 6 の CPU 5 3 は、乱数  $Na$  及び乱数  $Nb$  に、鍵  $K'ab$  を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、乱数  $R1$  を求める。ステップ S 4 8 9 において、ポータブルデバイス 6 の CPU 5 3 は、乱数  $Sb$  を生成する。

ステップ S 4 9 0 において、ポータブルデバイス 6 の CPU 5 3 は、USB コントローラ 5 7 に、ポータブルデバイス 6 の ID、乱数  $Nb$ 、乱数  $R1$ 、鍵番号  $j$  及び乱数  $Sb$  をパーソナルコンピュータ 1 へ送信させる。

ステップ S 4 5 3 において、パーソナルコンピュータ 1 は、インターフェース 1 7 を介して、ポータブルデバイス 6 の ID、乱数  $Nb$ 、乱数  $R1$ 、鍵番号  $j$  及び乱数  $Sb$  を受信する。ステップ S 4 5

4において、パーソナルコンピュータ1のCPU11は、ポータブルデバイス6のIDに、パーソナルコンピュータ1のマスター鍵KMPを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵Kmを求める。ステップS455において、パーソナルコンピュータ1のCPU11は、j番目の個別鍵KIaを求める。ステップS456において、パーソナルコンピュータ1のCPU11は、乱数Na及び乱数Nbに、鍵KIaを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'abを求める。ステップS457において、パーソナルコンピュータ1のCPU11は、乱数Na及び乱数Nbに、鍵K'abを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R2を求める。

ステップS458において、パーソナルコンピュータ1のCPU11は、受信した乱数R1と、ステップS457で生成した乱数R2とが等しいか否かを判定し、乱数R1と乱数R2とが等しくないと判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス6を認証せず、処理は終了する。ステップS458において、乱数R1と乱数R2とが等しいと判定された場合、ポータブルデバイス6は正当なポータブルデバイスなので、ステップS459に進み、パーソナルコンピュータ1のCPU11は、乱数Saを生成する。

ステップS460において、パーソナルコンピュータ1のCPU11は、乱数Nb及び乱数Naに、鍵KIaを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R3を求める。ステップS461において、パーソナルコンピュータ1のCPU1

1 は、インターフェース 17 を介して、ポータブルデバイス 6 に、乱数 R 3 及び乱数 S b を送信する。ステップ S 4 6 2 において、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 S a 及び乱数 S b に、鍵 K' a b を基にした S H A などのハッシュ関数を適用ハッシュ関数を適用し、一時鍵 K s を求める。

ステップ S 4 9 1 において、ポータブルデバイス 6 の CPU 5 3 は、乱数 R 3 及び乱数 S b を受信する。ステップ S 4 9 2 において、ポータブルデバイス 6 の CPU 5 3 は、乱数 N b 及び乱数 N a に、鍵 K a b を基にした S H A などのハッシュ関数を適用ハッシュ関数を適用し、乱数 R 4 を求める。ステップ S 4 9 3 において、ポータブルデバイス 6 の CPU 5 3 は、受信した乱数 R 3 と、ステップ S 4 9 2 で生成した乱数 R 4 とが等しいか否かを判定し、乱数 R 3 と乱数 R 4 とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ 1 を認証せず、処理は終了する。ステップ S 4 9 3 において、乱数 R 3 と乱数 R 4 とが等しいと判定された場合、パーソナルコンピュータ 1 は、正当なパーソナルコンピュータなので、ステップ S 4 9 4 に進み、ポータブルデバイス 6 の CPU 5 3 は、乱数 S a 及び乱数 S b に、鍵 K a b を基にした S H A などのハッシュ関数を適用ハッシュ関数を適用し、一時鍵 K s を求める。

このように、パーソナルコンピュータ 1 及びポータブルデバイス 6 は、相互認証し、共通の一時鍵 K s を得る。図 4 0 及び図 4 1 のフローチャートに示した手続は、図 3 8 及び図 3 9 のフローチャートに示す手続よりも、いわゆる”なりすまし”に対する防御（検出）が強力である。なお、ステップ S 4 8 5、ステップ S 4 8 7、

ステップS 4 8 8、ステップS 4 5 4、ステップS 4 5 6、ステップS 4 5 7、ステップS 4 6 0、ステップS 4 6 2、ステップS 4 9 2及びステップS 4 9 4において、SHAなどのハッシュ関数を適用するとして説明したが、DESなどを適用しても良い。

以上のように、パーソナルコンピュータ1及びポータブルデバイス6は、相互認証の後に行われる処理に対応し、検出力が異なる相互認証の手続を使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

次に、ソースプログラムを暗号化する処理を、図42のフローチャートを参照して説明する。ステップS 5 0 1において、パーソナルコンピュータ1は、通信部25を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップS 5 0 2において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

ステップS 5 0 2において、受信したソースプログラムに改竄が発見されなかった場合、ステップS 5 0 3に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップS 5 0 4において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ1に送信する。ステップS 5 0 5において、パーソナルコンピュータ1は、受信したソースプログラムを、HDD21に記録し、処理は終了する。

以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、EMDサーバ4-1乃至4-3又は所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

次に、暗号化されたソースプログラムをアダプタ 26 が実行する処理を、図 43 のフローチャートを参照して説明する。ステップ S 521 において、アダプタ 26 の CPU 32 は、パーソナルコンピュータ 1 から受信した、暗号化されたソースプログラムを、不揮発性メモリ 34 に予め記憶されている認証局の公開鍵で復号する。ステップ S 522 において、アダプタ 26 の CPU 32 は、インタプリタを起動し、復号されたソースプログラムを実行する。

ステップ S 523 において、アダプタ 26 の CPU 32 は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ 1 に送信するか否かを判定し、結果をパーソナルコンピュータ 1 に送信しないと判定された場合、処理は終了する。ステップ S 523 において、結果をパーソナルコンピュータ 1 に送信すると判定された場合、ステップ S 524 に進み、アダプタ 26 の CPU 32 は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップ S 525 において、アダプタ 26 の CPU 32 は、インターフェース 31 を介して、暗号化された結果をパーソナルコンピュータ 1 に送信し、処理は終了する。

以上のように、アダプタ 26 は、暗号化されたソースプログラムを実行し、所定の場合、得られた結果を暗号化し、パーソナルコンピュータ 1 に送信する。

なお、オブジェクトプログラムを暗号化し、暗号化されたオブジェクトプログラムをアダプタ 26 が実行するようにしてもよい。図 44 は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップ S 541 において、パーソナルコンピュータ 1 は、ソースプログラムをコンパイルし、所定のオブジェク



トプログラムを生成する。ステップS 5 4 2乃至ステップS 5 4 6の処理は、図4 2のステップS 5 0 1乃至ステップS 5 0 5とそれぞれ同様の処理なので、その説明は省略する。

図4 5は、暗号化されたオブジェクトプログラムをアダプタ2 6が実行する処理を説明するフローチャートである。ステップS 5 6 1において、アダプタ2 6のCPU 3 2は、パーソナルコンピュータ1から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ3 4に予め記憶されている認証局の公開鍵で復号する。ステップS 5 6 2において、アダプタ2 6のCPU 3 2は、復号されたオブジェクトプログラムをRAM 3 3に展開し、実行する。ステップS 5 6 3乃至ステップS 5 6 5は、図4 3のステップ5 2 3乃至ステップS 5 2 5とそれぞれ同様の処理なので、その説明は省略する。

次に、オブジェクトプログラムを暗号化する他の処理を、図4 6のフローチャートを参照して説明する。ステップS 5 8 1において、パーソナルコンピュータ1のCPU 1 1は、ソースプログラムをコンパイルし、オブジェクトプログラムを生成する。ステップS 5 8 2において、パーソナルコンピュータ1のCPU 1 1は、インターフェース1 7を介して、アダプタ2 6にアプリケーション鍵K a p及び個別鍵K i d vの発行を要求する。

ステップS 5 8 3において、パーソナルコンピュータ1は、インターフェース1 7を介して、アダプタ2 6からアプリケーション鍵K a p及び個別鍵K i d v（アダプタ2 6の不揮発性メモリ3 4に記憶されている、アダプタ2 6固有の鍵K sを基に、生成される）を受信する。ステップS 5 8 4において、パーソナルコンピュータ

1のCPU11は、オブジェクトプログラムをアプリケーション鍵K<sub>ap</sub>で暗号化する。ステップS585において、パーソナルコンピュータ1のCPU11は、コンテキストに含まれるマスター鍵K<sub>Mb</sub>などを個別鍵K<sub>idv</sub>で暗号化する。ステップS586において、パーソナルコンピュータ1のCPU11は、アプリケーション鍵K<sub>ap</sub>で暗号化されたオブジェクトプログラム及び個別鍵K<sub>idv</sub>で暗号化されたコンテキストに含まれるマスター鍵K<sub>Mb</sub>などをHDD21に記録させ、処理は終了する。

このように、パーソナルコンピュータ1は、アダプタ26から供給されたアプリケーション鍵K<sub>ap</sub>及び個別鍵K<sub>idv</sub>で、オブジェクトプログラム及びコンテキストを暗号化することができる。

図46のフローチャートに示される手順で暗号化されたオブジェクトプログラムをアダプタ26が実行する処理を、図47のフローチャートを参照して説明する。ステップS601において、パーソナルコンピュータ1のCPU11は、インターフェース17を介して、アダプタ26に、アプリケーション鍵K<sub>ap</sub>で暗号化されたオブジェクトプログラム及び個別鍵K<sub>idv</sub>で暗号化されたコンテキストに含まれるマスター鍵K<sub>Mb</sub>などを送信する。

ステップS602において、アダプタ26のCPU32は、不揮発性メモリ34に予め記憶されている鍵K<sub>s</sub>及びアプリケーション鍵K<sub>ap</sub>に、ハッシュ関数を適用し、個別鍵K<sub>idv</sub>を生成する。ステップS603において、アダプタ26のCPU32は、受信したオブジェクトプログラムをアプリケーション鍵K<sub>ap</sub>で復号する。ステップS604において、アダプタ26のCPU32は、コンテキストに含まれるマスター鍵K<sub>Mb</sub>などを個別鍵K<sub>idv</sub>で復号す

る。

ステップS 6 0 5において、アダプタ2 6のCPU 3 2は、復号されたマスター鍵K M bなどを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップS 6 0 6乃至ステップS 6 0 8の処理は、図4 3のステップS 5 2 3乃至ステップS 5 2 5とそれぞれ同様なので、その説明は省略する。

以上のように、図4 7のフローチャートで示される処理において、図4 6のフローチャートで個別鍵K i d vを送信したアダプタ2 6は、暗号化されたオブジェクトプログラムを実行することができる。従って、図4 6のフローチャートで個別鍵K i d vを送信したアダプタ2 6以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

次に、アダプタ2 6がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ1のCPU 1 1に実行させるときの処理を図4 8のフローチャートを参照して説明する。ステップS 6 5 1において、アダプタ2 6のCPU 3 2は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

この変換は、例えば、DESの暗号化又は復号のプログラムの場合、Feistel 構造などの基本構造を繰り返す処理のとき、いわゆるF関数で利用される4 8ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、DES CBC(Cipher Block Chaining) Modeで、多量のデータを復号するプログラムの場合、繰り返し構造の処理を順(シーケンシャル)に実行せず、多量のデータ

に対し、複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

また、例えば、ソースプログラムのインストラクションに対応するコード（例えば、加算を表すコードが” 1 ”に対応し、乗算を表すコードが” 2 ”に対応する）を毎回変更する。

ステップ S 6 5 2 において、アダプタ 2 6 の CPU 3 2 は、変換された命令列を、インターフェース 3 1 を介して、パーソナルコンピュータ 1 に送信する。

ステップ S 6 5 3 において、パーソナルコンピュータ 1 の CPU 1 1 は、デシャッフルされた命令列を実行する。ステップ S 6 5 4 において、パーソナルコンピュータ 1 の CPU 1 1 は、命令列を実行して得られた処理結果をアダプタ 2 6 に送信する。

ステップ S 6 5 5 において、アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 から受信した処理結果及びアダプタ 2 6 の CPU 3 2 が算出し保持している計算結果を基に、処理を継続する。ステップ S 6 5 6 において、アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 に処理を実行させるか否かを判定し、パーソナルコンピュータ 1 に処理を実行させないと判定された場合、処理は終了する。ステップ S 6 5 6 において、パーソナルコンピュータ 1 に処理を実行させると判定された場合、手続は、ステップ S 6 5 1 に戻り、パーソナルコンピュータ 1 に処理を実行させる処理を繰り返す。

以上のように、アダプタ 2 6 は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ 1 に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することがで

きる。

アダプタ 26 は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ 1 に送信することにより、オブジェクトプログラムの解読が困難になる。アダプタ 26 が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ 1 に送信すれば、オブジェクトプログラムの解読は更に困難になる。

なお、図 46 で説明したパーソナルコンピュータ 1 がアダプタ 26 に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対しステップ S651 に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

最後に、パーソナルコンピュータ 1 が EMD サーバ 4-1 乃至 4-3 から、事前に無料でダウンロードした音楽データを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図 49 のフローチャートを参照して説明する。ステップ S671 において、パーソナルコンピュータ 1 は、ネットワーク 2 を介して EMD サーバ 4-1 乃至 4-3 と相互認証する。ステップ S672 において、パーソナルコンピュータ 1 の CPU 11 は、通信部 25 を介して、EMD サーバ 4-1 乃至 4-3 に、音楽データの再生条件を示すデータを送信する。ステップ S673 において、EMD サーバ 4-1 乃至 4-3 は、受信した再生条件を示すデータを基に、支払金額のデータをパーソナルコンピュータ 1 に送信する。

ステップ S674 において、パーソナルコンピュータ 1 の CPU 11 は、EMD サーバ 4-1 乃至 4-3 から受信した支払金額のデータをディスプレイ 20 に表示させる。ステップ S675 において、

EMDサーバ4-1乃至4-3は、パーソナルコンピュータ1に、ユーザのクレジットカードの番号等の送信を要求する。ステップS676において、ユーザは、キーボード18又はマウス19を操作し、パーソナルコンピュータ1にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ1は、クレジットカードの番号等のデータをEMDサーバ4-1乃至4-3に送信する。

ステップS677において、EMDサーバ4-1乃至4-3は、パーソナルコンピュータ1から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。ステップS678において、EMDサーバ4-1乃至4-3は、ネットワーク2を介して、パーソナルコンピュータ1に所定の暗号鍵を送信する。ステップS679において、パーソナルコンピュータ1は、ネットワーク2を介して、EMDサーバ4-1乃至4-3から送信された所定の暗号鍵を受信し、処理は終了する。

以上のように、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3から暗号鍵をダウンロードするとともに、EMDサーバ4-1乃至4-3は、決済の処理をすれば、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3から音楽データをダウンロードするとき、認証、暗号化、又は決済などの処理が必要なくなるので、比較的大きなデータである音楽データを迅速にダウンロードすることができる。

以上においては、記録媒体として、ポータブルデバイス6を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行するとし

て説明したが、s m a s h（商標）などの手続により、決済をするようにしてもよい。

また、図49のフローチャートに示す処理の前に、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3とが、例えば、ISO 9798-3で規定されているhttp(Hypertext Transport Protocol)上のプロトコルを使用して、相互認証するようにしてもよい。

なお、ポータブルデバイス6は、予め個別鍵を記憶しているとして説明したが、ユーザがポータブルデバイス6を購入後、EMDサーバ4-1乃至4-3などからダウンロードするようにしてもよい。

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

以上においては、記録媒体として、ポータブルデバイス6を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。また、コンテンツは、曲のデータ又は音声データなどの楽音データ以外に、画像データ、その他のデータとすることもできる。

このように、本発明によれば、次のような効果を奏することができる。

(1) HDD 21に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でHDD 21に記録するようにしたので、HDD 21に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

(2) 所定の曲を1回コピーしたとき、一定時間（上記例の場

合、48時間)の間、その曲をコピーすることができないようにするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

さらにデータベースを更新するたびに、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

(3) 外部の装置にコンテンツを渡したら、HDD 21上のコンテンツを消去するようにしたので、HDD 21内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

(4) HDD 21内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD 21の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD 21にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

(7) 曲の同一性の判定にISRCを用い、ISRCが取得で



きないときは、T O Cを用いるようにしたので、I S R Cが取得できなくとも、曲の同一性を判定することが可能になる。

(8) パーソナルコンピュータ 1 におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ 1 に外付けされるアダプタ 2 6 に負担させるようにしたので、パーソナルコンピュータ 1 のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

更に、そのソフトウェアが、安全な認証局又は E M D サーバ 4 - 1 乃至 4 - 3 で暗号化又はシャッフルされるので、ソフトウェアの改竄は、より困難となる。

(9) プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ 2 6 が生成する固有の鍵で暗号化するようにしたので、プログラムのみを C D - R O M などの媒体で配布可能にしつつ、プログラムを他のアダプタ 2 6 で実行することが防止される。

(10) 音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

なお、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、C D - R O M、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体

を利用することができる。

以上のように、本発明に係る情報提供装置、情報提供方法及びプログラム提供媒体では、情報処理装置から所定のプログラムが受信されるとともに、暗号化されたプログラムが情報処理装置に送信され、受信したプログラムが暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理が選択され、選択された相互認証の手続が実行されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報提供装置、情報提供方法及びプログラム提供媒体では、情報処理装置から、情報処理装置がダウンロードしたデータの利用に関するデータ及び決済に必要なデータが受信されるとともに、情報処理装置に、鍵が送信され、情報処理装置から受信したデータの利用に関するデータ及び決済に必要なデータを基に、決済されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体によれば、暗号化されているプログラムが復号され実行され、プログラムが供給されるとともに、暗号化されているプログラムが復号され、実行の結果を基に、プログラムが実行されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体 I C に実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 I C に送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理システムでは、半導体 I C に実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 I C に送信され、半導体 I C に実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体 I C に実行させるプログラムに含まれる命令列が並び替えられ、命令列が並び替えられたプログラムが記録され、記録されているプログラムが、半導体 I C に送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体 I C に実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えら

れ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 I C に送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、プログラム及びプログラムの実行に必要なデータが蓄積され、プログラム及びデータの蓄積又は読み出しが制御され、プログラムが半導体 I C から供給された第 1 の鍵で暗号化され、データが半導体 I C から供給された第 2 の鍵で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る半導体 I C、情報処理方法及びプログラム提供媒体によれば、情報処理装置から転送されてくる暗号化されている第 1 のプログラムが受信され、受信された第 1 のプログラムが復号され、復号された第 1 のプログラムを処理する第 2 のプログラムが保持され、保持されている第 2 のプログラムに基づいて処理された第 1 のプログラムが実行され、実行した結果が情報処理装置に転送され、計時動作を行うとともに、情報処理装置からの時刻情報に基づいて、現在時刻が修正されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体 I C に暗号化されているプログラムが送信され、半導体 I C が、プログラムを処理した結果生成し、出力したデータが受信され、他の装置からデータと時刻情報が受信され、受信したデータが蓄積され、受信した時刻情報に基づいて、半導体 I C

の時刻情報が修正されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る半導体 I C、情報処理方法、プログラム提供媒体では、半導体 I C 固有の第 1 の鍵が予め記憶され、記憶している第 1 の鍵及び情報処理装置から供給されたプログラムの属性から、第 2 の鍵が生成され、プログラムが第 3 の鍵で復号され、データが第 2 の鍵で復号されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

さらに、本発明に係る情報処理システムによれば、プログラム及びプログラムの実行に必要なデータが蓄積され、プログラム及びデータの蓄積又は読み出しが制御され、プログラムが半導体 I C から供給された第 1 の鍵で暗号化され、データが半導体 I C から供給された第 2 の鍵で暗号化され、暗号化されたプログラム及びプログラムの実行に必要なデータが半導体 I C に送信されるとともに、第 1 の鍵及び第 2 の鍵が半導体 I C から受信され、暗号化されたプログラム及びプログラムの実行に必要なデータが受信されるとともに、第 1 の鍵及び第 2 の鍵が情報処理装置に送信され、半導体 I C 固有の第 3 の鍵が予め記憶され、記憶している第 3 の鍵及び情報処理装置から供給されたプログラムの属性から、第 2 の鍵が生成され、受信したプログラムが第 1 の鍵で復号され、受信したデータが第 2 の鍵で復号されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

### 請求の範囲

1. ネットワークを介して、所定の情報処理装置に接続されている情報提供装置において、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信手段と、

通信手段が受信した前記プログラムを暗号化する暗号化手段とを含むことを特徴とする情報提供装置。

2. 前記プログラムは、インタプリタに実行させるソースプログラムであることを特徴とする請求の範囲第1項に記載の情報提供装置。

3. 前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第1項に記載の情報提供装置。

4. ネットワークを介して、所定の情報処理装置に接続されている情報提供装置の情報提供方法において、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、

通信ステップで受信した前記プログラムを暗号化する暗号化ステップと

を含むことを特徴とする情報提供方法。

5. ネットワークを介して、所定の情報処理装置に接続されている情報提供装置に、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、

通信ステップで受信した前記プログラムを暗号化する暗号化ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

6. 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置において、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択手段と、

前記選択手段が選択された相互認証の手続を実行する相互認証手段と

を含むことを特徴とする情報処理装置。

7. 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置の情報処理方法において、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、

前記選択ステップで選択された相互認証の手続を実行する相互認証ステップと

を含むことを特徴とする情報処理方法。

8. 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置に、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、

前記選択ステップで選択された相互認証の手続を実行する相互認証ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

9. 第1装置において第1乱数を発生し、

第1装置の識別情報と鍵の属性情報と上記第1乱数とを第1装置から第2装置に送信し、

第2装置において第2乱数を発生し、

第2装置において上記第1装置から送信された第1装置の識別情報と鍵の属性情報と第1乱数とを受信し、

第2装置において上記鍵の属性情報から鍵を計算し、

第2装置において上記鍵と上記第1・第2乱数から第3乱数を発生し、

第2・第3乱数と鍵に関する情報とを第2装置から第1装置に送信し、

第1装置において上記第2装置から送信された第2・第3乱数と鍵に関する情報とを受信し、

第1装置において上記鍵に関する情報から鍵を生成し、

第1装置において上記鍵と上記第1・第2乱数から第4乱数を発生し、

上記第4乱数を第1装置から第2装置に送信し、

第1・第2装置の各々において第3・第4乱数と鍵とから一時鍵を求めることを特徴とする認証方法。

10. 第1装置において第1乱数を発生し、

第1装置の識別情報と第1装置の鍵の属性情報と第2装置の鍵の



属性情報と上記第 1 乱数とを第 1 装置から第 2 装置に送信し、

第 2 装置において第 2 乱数を発生し、

第 2 装置において上記第 1 装置から送信された第 1 装置の識別情報と鍵の属性情報と第 2 装置の鍵の属性情報と上記第 1 乱数とを受信し、

第 2 装置において上記第 2 装置の鍵の属性情報から第 1 鍵を計算し、

第 2 装置において上記第 1 装置の鍵の属性情報から第 2 鍵を計算し、

第 2 装置において上記第 2 鍵と上記第 1・第 2 乱数から第 3 乱数を発生し、

第 2・第 3 乱数と鍵に関する情報とを第 2 装置から第 1 装置に送信し、

第 1 装置において上記第 2 装置から送信された第 2・第 3 乱数と鍵に関する情報とを受信し、

第 1 装置において上記鍵に関する情報から第 2 鍵を生成し、

第 1 装置において上記第 2 鍵と上記第 1・第 2 乱数から第 4 乱数を発生し、

上記第 4 乱数を第 1 装置から第 2 装置に送信し、

第 1・第 2 装置の各々において第 3・第 4 乱数と第 2 鍵とから一時鍵を求めることを特徴とする認証方法。

11. 暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置において、

前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信する

とともに、前記情報処理装置に、前記鍵を送信する通信手段と、

前記情報処理装置から受信した前記データの利用に関するデータ  
及び決済に必要なデータを基に、決済をする決済手段と

を含むことを特徴とする情報提供装置。

12. http上のプロトコルを利用して、前記情報処理装置と  
相互認証する相互認証手段を更に含むことを特徴とする請求の範囲  
第11項に記載の情報提供装置。

13. 暗号化されている所定のデータ及び前記所定のデータを暗  
号化している鍵を情報処理装置に提供する情報提供装置の情報提供  
方法において、

前記情報処理装置から、前記情報処理装置がダウンロードした前  
記データの利用に関するデータ及び決済に必要なデータを受信する  
とともに、前記情報処理装置に、前記鍵を送信する通信ステップと、

前記情報処理装置から受信した前記データの利用に関するデータ  
及び決済に必要なデータを基に、決済をする決済ステップと

を含むことを特徴とする情報提供方法。

14. 暗号化されている所定のデータ及び前記所定のデータを暗  
号化している鍵を情報処理装置に提供する情報提供装置に、

前記情報処理装置から、前記情報処理装置がダウンロードした前  
記データの利用に関するデータ及び決済に必要なデータを受信する  
とともに、前記情報処理装置に、前記鍵を送信する通信ステップと、

前記情報処理装置から受信した前記データの利用に関するデータ  
及び決済に必要なデータを基に、決済をする決済ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラ  
ムを提供することを特徴とするプログラム提供媒体。

15. 暗号化されているプログラムを復号して実行する第1の実行手段と、

前記プログラムを前記第1の実行手段に供給するとともに、暗号化されている前記プログラムを復号し、前記第1の実行手段の実行の結果を基に、前記プログラムを実行する第2の実行手段と

を含むことを特徴とする情報処理装置。

16. 前記第1の実行手段及び前記第2の実行手段は、それぞれ独立したハードウェアに設けられていることを特徴とする請求項15に記載の情報処理装置。

17. 前記プログラムは、インタプリタに実行させるソースプログラムであることを特徴とする請求の範囲第15項に記載の情報処理装置。

18. 前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第15項に記載の情報処理装置。

19. 暗号化されているプログラムを復号して実行する第1の実行ステップと、

前記プログラムを前記第1の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第1の実行ステップの実行の結果を基に、前記プログラムを実行する第2の実行ステップと

を含むことを特徴とする情報処理装置の情報処理方法。

20. 暗号化されているプログラムを復号して実行する第1の実行ステップと、

前記プログラムを前記第1の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第1の実行ステッ

プの実行の結果を基に、前記プログラムを実行する第2の実行ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

21. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置において、

前記半導体ICに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ICに送信する送信手段と

を含むことを特徴とする情報処理装置。

22. 前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第21項に記載の情報処理装置。

23. 前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第21項に記載の情報処理装置。

24. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ICに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録す

る記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップと

を含むことを特徴とする情報処理方法。

25. 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、

前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

26. 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置及び認証局からなる情報処理システムにおいて、

前記情報処理装置は、前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含み、

前記認証局は、前記半導体 I C に実行させる前記プログラムを受

信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段とを含む

ことを特徴とする情報処理システム。

27. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置において、

前記半導体ICに実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、

前記命令列が並び替えられた前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ICに送信する送信手段と

を含むことを特徴とする情報処理装置。

28. 前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第27項に記載の情報処理装置。

29. 前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第27項に記載の情報処理装置。

30. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ICに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記命令列が並び替えられた前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導

体 I C に送信する送信ステップと

を含むことを特徴とする情報処理方法。

31. 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、

前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記命令列が並び替えられた前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

32. 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、

前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、

前記プログラムを暗号化する暗号化手段と、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段と

を含むことを特徴とする情報処理装置。

33. 前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第32項に記載の情報処理装置。

34. 前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第32項に記載の情報処理装置。

35. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ICに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ICに送信する送信ステップと

を含むことを特徴とする情報処理方法。

36. 半導体ICが装着され、前記半導体ICに実行させるプログラムを供給する情報処理装置に、

前記半導体ICに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ICに送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

37. 情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ICにおいて、



前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信手段と、

前記受信手段により受信された前記第 1 のプログラムを復号する復号手段と、

前記復号手段により復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持手段と、

前記保持手段に保持されている前記第 2 のプログラムに基づいて処理された前記第 1 のプログラムを実行する実行手段と、

前記実行手段が実行した結果を前記情報処理装置に転送する転送手段と、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時手段と

を含むことを特徴とする半導体 IC。

38. 前記情報処理装置が利用するデータを記憶する不揮発性の記憶手段をさらに含むことを特徴とする請求の範囲第 37 項に記載の半導体 IC。

39. 情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体 IC の情報処理方法において、

前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信ステップと、

前記受信ステップで受信された前記第 1 のプログラムを復号する復号ステップと、

前記復号ステップで復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持ステップと、

前記保持ステップの処理で保持された前記第 2 のプログラムに基

づいて処理された前記第 1 のプログラムを実行する実行ステップと、  
前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップと

を含むことを特徴とする情報処理方法。

40. 情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体 IC に、

前記情報処理装置から転送されてくる暗号化されている第 1 のプログラムを受信する受信ステップと、

前記受信ステップで受信された前記第 1 のプログラムを復号する復号ステップと、

前記復号ステップで復号された前記第 1 のプログラムを処理する第 2 のプログラムを保持する保持ステップと、

前記保持ステップの処理で保持された前記第 2 のプログラムに基づいて処理された前記第 1 のプログラムを実行する実行ステップと、

前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

41. 装着された半導体 IC に各種の指令を出力し、実行させる情報処理装置において、

前記半導体 IC に暗号化されているプログラムを送信する送信手

段と、

前記半導体 I C が、前記プログラムを処理した結果生成し、出力したデータを受信する第 1 の受信手段と、

他の装置からデータと時刻情報を受信する第 2 の受信手段と、

前記第 2 の受信手段が受信したデータを蓄積する蓄積手段と、

前記第 2 の受信手段が受信した時刻情報に基づいて、前記半導体 I C の時刻情報を修正させる修正手段と

を含むことを特徴とする情報処理装置。

4 2. 装着された半導体 I C に各種の指令を出力し、実行させる情報処理装置の情報処理方法において、

前記半導体 I C に暗号化されているプログラムを送信する送信ステップと、

前記半導体 I C が、前記プログラムを処理した結果生成し、出力したデータを受信する第 1 の受信ステップと、

他の装置からデータと時刻情報を受信する第 2 の受信ステップと、

前記第 2 の受信ステップで受信したデータを蓄積する蓄積ステップと、

前記第 2 の受信ステップで受信した時刻情報に基づいて、前記半導体 I C の時刻情報を修正させる修正ステップと

を含むことを特徴とする情報処理方法。

4 3. 装着された半導体 I C に各種の指令を出力し、実行させる情報処理装置に、

前記半導体 I C に暗号化されているプログラムを送信する送信ステップと、

前記半導体 I C が、前記プログラムを処理した結果生成し、出力

したデータを受信する第 1 の受信ステップと、

他の装置からデータと時刻情報を受信する第 2 の受信ステップと、

前記第 2 の受信ステップで受信したデータを蓄積する蓄積ステップと、

前記第 2 の受信ステップで受信した時刻情報に基づいて、前記半導体 I C の時刻情報を修正させる修正ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

4 4. 所定の半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、

前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、

前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化手段と、

前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化手段と

を含むことを特徴とする情報処理装置。

4 5. 前記第 1 の鍵は、前記プログラムの属性で決定されることを特徴とする請求の範囲第 4 4 項に記載の情報処理装置。

4 6. 前記第 2 の鍵は、前記プログラムの属性及び前記半導体 I C が予め記憶している第 3 の鍵で決定される

ことを特徴とする請求の範囲第 4 4 項に記載の情報処理装置。

4 7. 所定の半導体 I C が装着され、前記半導体 I C に実行させ

るプログラムを供給する情報処理装置の情報処理方法において、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、

前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、

前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化ステップと、

前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化ステップと

を含むことを特徴とする情報処理方法。

48. 所定の半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、

前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、

前記プログラムを前記半導体 I C から供給された第 1 の鍵で暗号化する第 1 の暗号化ステップと、

前記データを前記半導体 I C から供給された第 2 の鍵で暗号化する第 2 の暗号化ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

49. 所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体 I C において、

前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶手段と、  
前記記憶手段が記憶している前記第 1 の鍵及び前記情報処理装置  
から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成  
手段と、

前記プログラムを第 3 の鍵で復号する第 1 の復号手段と、  
前記データを第 2 の鍵で復号する第 2 の復号手段と  
を含むことを特徴とする半導体 I C。

50. 所定の情報処理装置に装着し、前記情報処理装置から供給  
されたプログラム及び前記プログラムの実行に必要なデータを受信  
し、前記プログラムを実行する半導体 I C の情報処理方法において、  
前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶ステップ  
と、

前記記憶ステップで記憶している前記第 1 の鍵及び前記情報処理  
装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵  
生成ステップと、

前記プログラムを第 3 の鍵で復号する第 1 の復号ステップと、  
前記データを第 2 の鍵で復号する第 2 の復号ステップと  
を含むことを特徴とする情報処理方法。

51. 所定の情報処理装置に装着し、前記情報処理装置から供給  
されたプログラム及び前記プログラムの実行に必要なデータを受信  
し、前記プログラムを実行する半導体 I C に、

前記半導体 I C 固有の第 1 の鍵を予め記憶している記憶ステップ  
と、

前記記憶ステップで記憶している前記第 1 の鍵及び前記情報処理  
装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵

生成ステップと、

前記プログラムを第 3 の鍵で復号する第 1 の復号ステップと、

前記データを第 2 の鍵で復号する第 2 の復号ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

52. 半導体 IC に実行させるプログラムを供給する情報処理装置及び前記情報処理装置に装着され、前記情報処理装置から供給されたプログラムを受信し、前記プログラムを実行する半導体 IC からなる情報処理システムにおいて、

前記情報処理装置は、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体 IC から供給された第 1 の鍵で暗号化する第 1 の暗号化手段と、前記データを前記半導体 IC から供給された第 2 の鍵で暗号化する第 2 の暗号化手段と、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記半導体 IC に送信するとともに、前記第 1 の鍵及び前記第 2 の鍵を前記半導体 IC から受信する第 1 の通信手段とを含み、

前記半導体 IC は、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記情報処理装置から受信するとともに、前記第 1 の鍵及び前記第 2 の鍵を前記情報処理装置に送信する第 2 の通信手段と、前記半導体 IC 固有の第 3 の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第 3 の鍵及び前記情報処理装置から供給されたプログラムの属性から、第 2 の鍵を生成する鍵生成手段と、前記第 2 の通信手段が受信した、前記プロ

グラムを第 1 の鍵で復号する第 1 の復号手段と、前記第 2 の通信手段が受信した、前記データを第 2 の鍵で復号する第 2 の復号手段とを含む

ことを特徴とする情報処理システム。



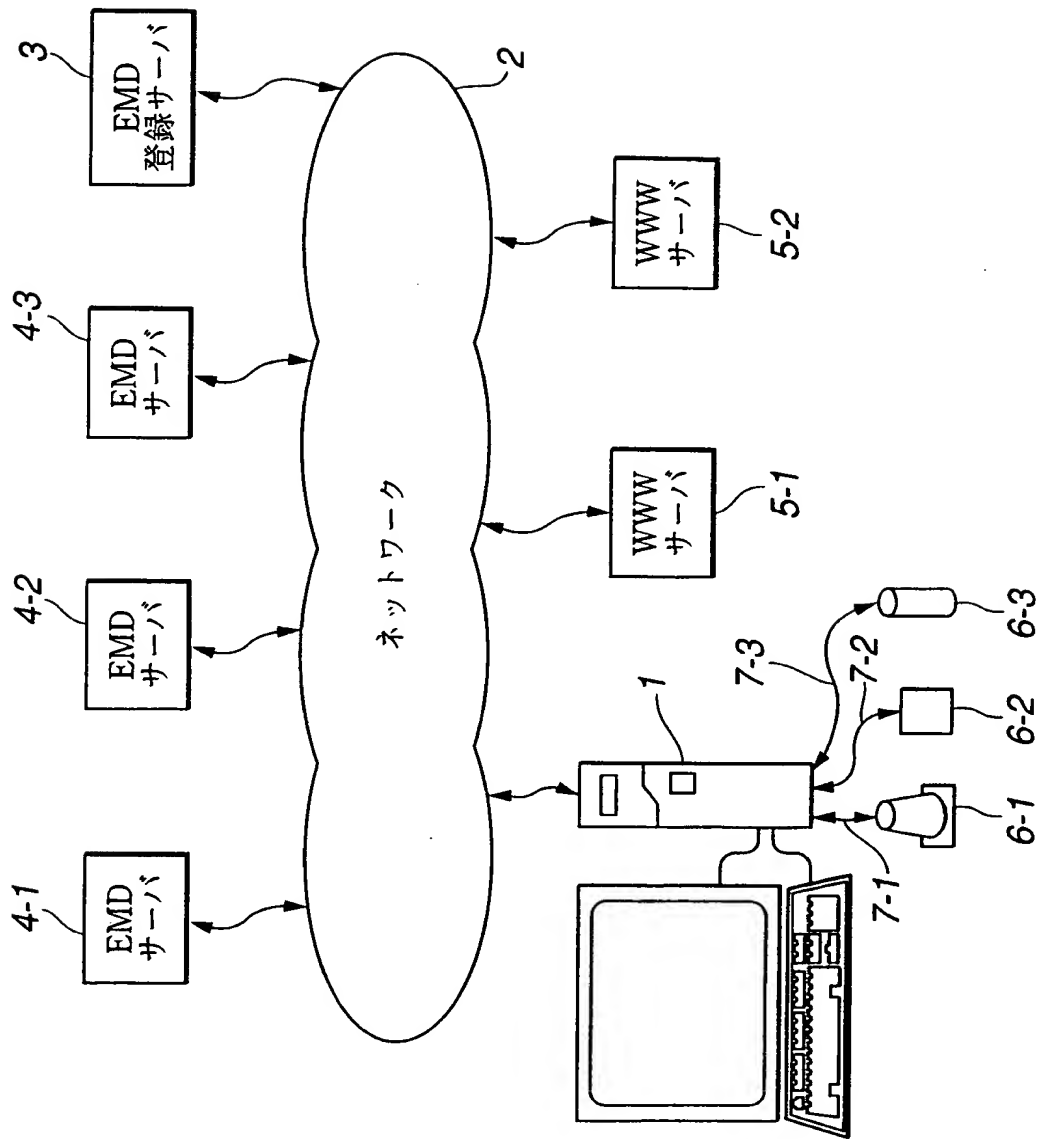


FIG.1

**THIS PAGE BLANK (USPTO)**

2/48

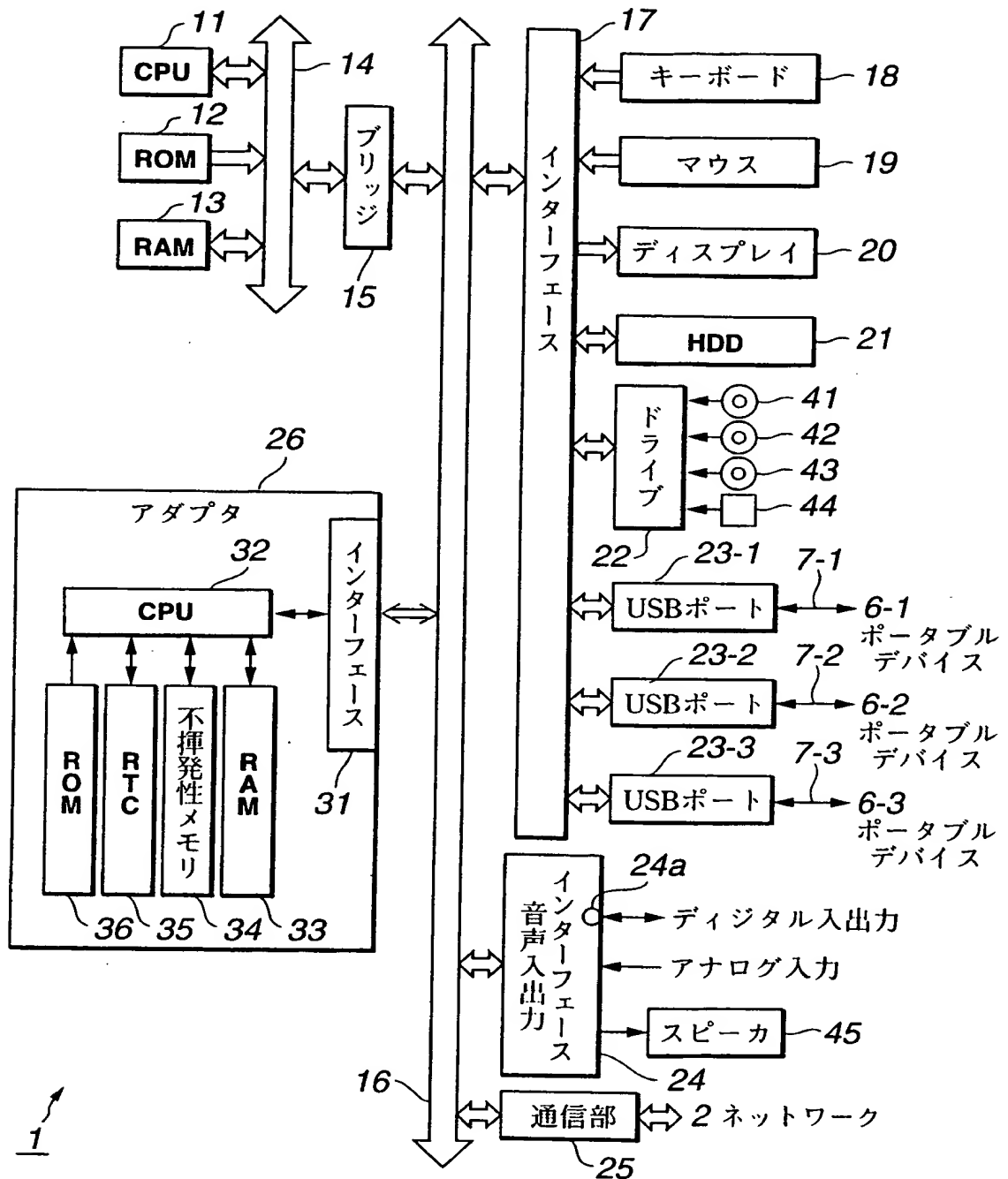


FIG.2

**THIS PAGE BLANK (USPTO)**

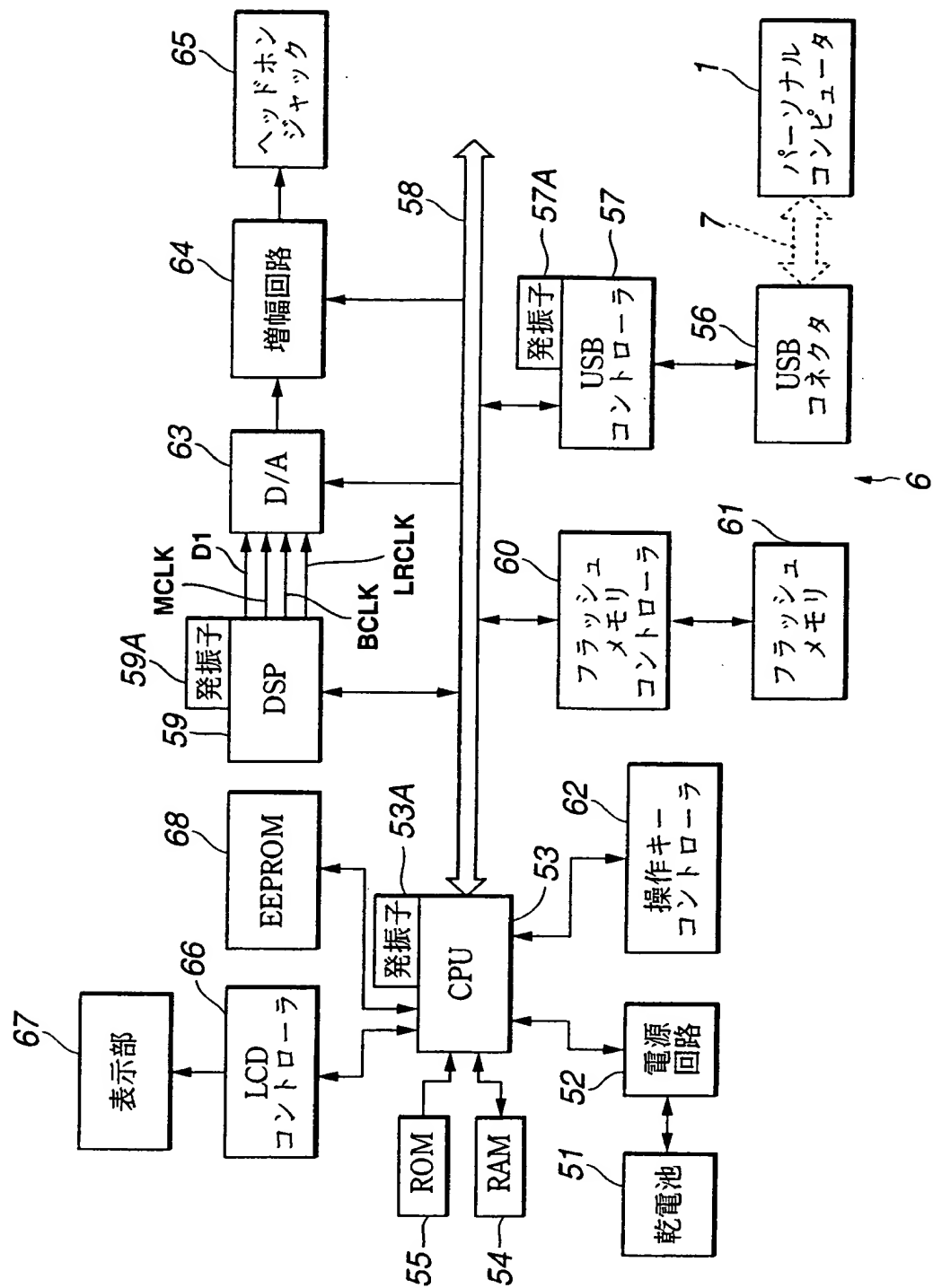


FIG.3

**THIS PAGE BLANK (USPTO)**

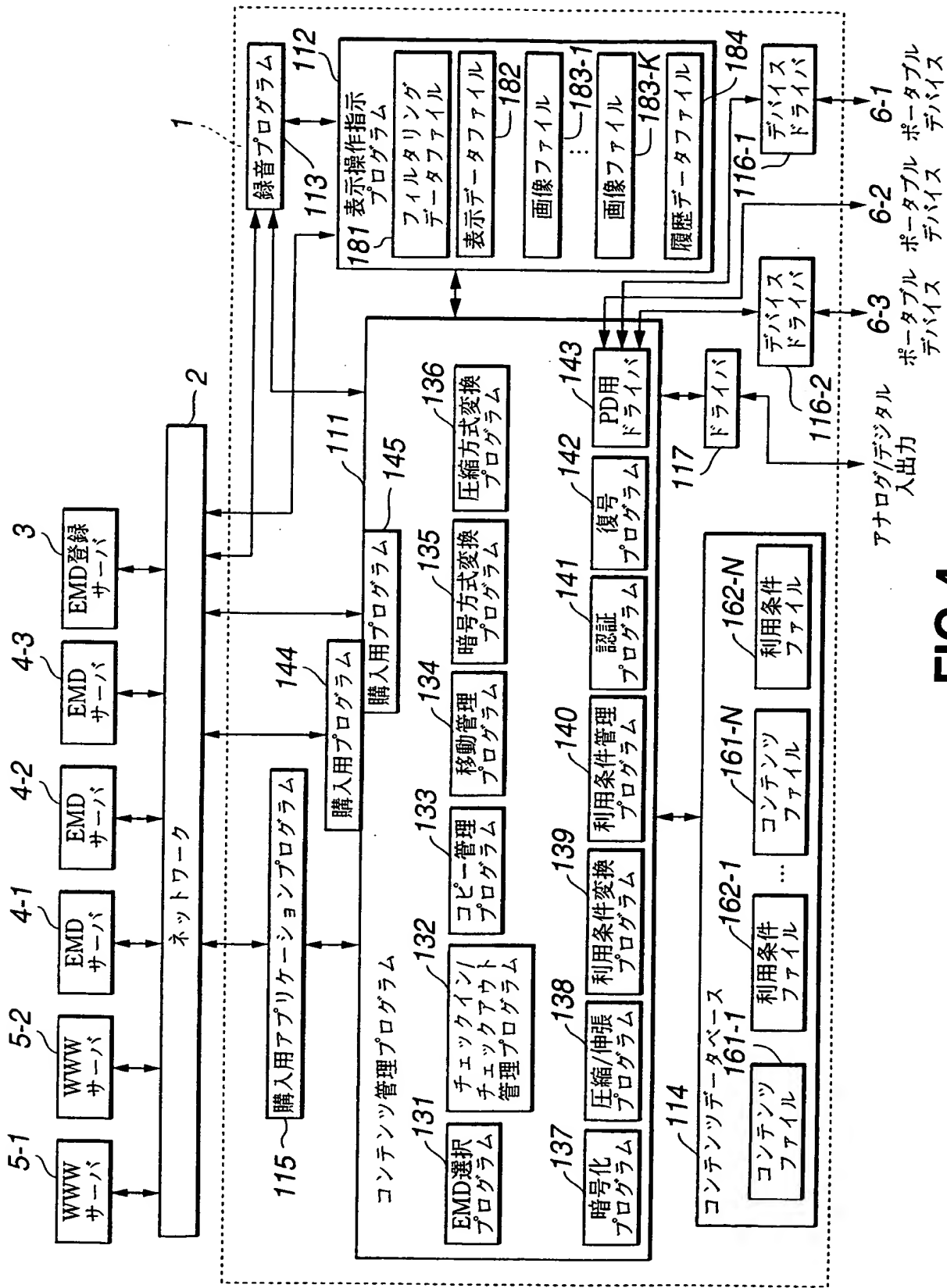


FIG.4

**THIS PAGE BLANK (USPTO)**



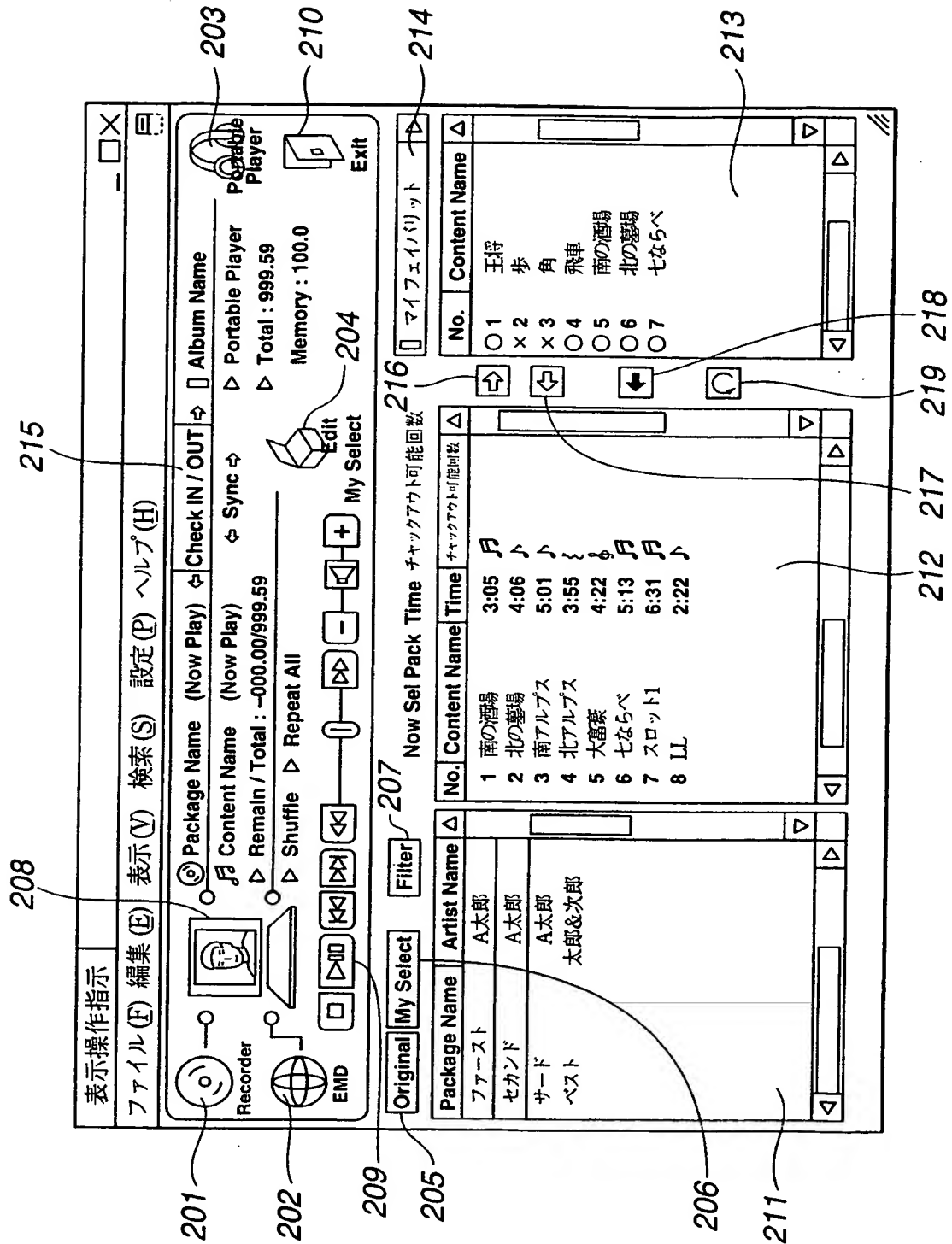


FIG. 5

**THIS PAGE BLANK (USPTO)**

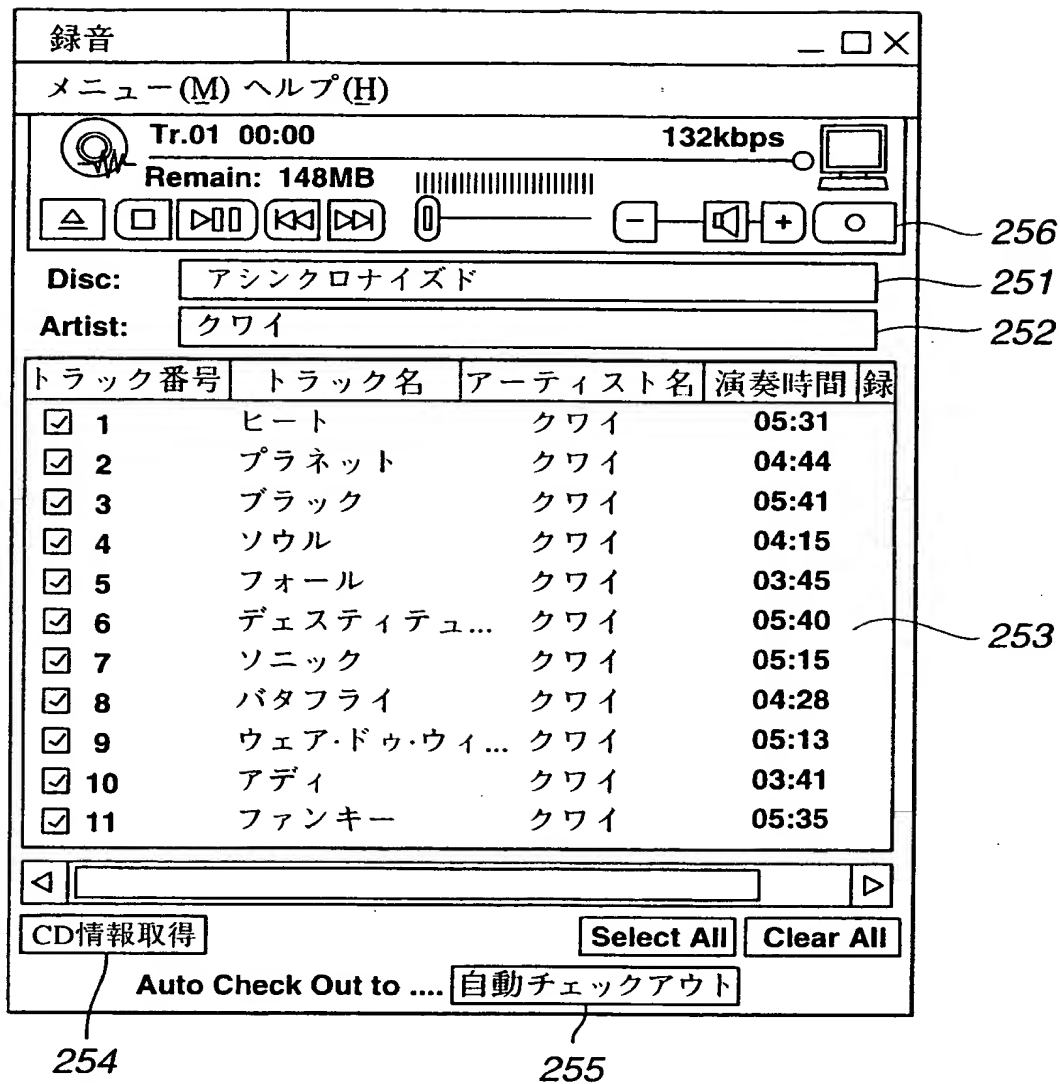


FIG.6

**THIS PAGE BLANK (USPTO)**

7/48

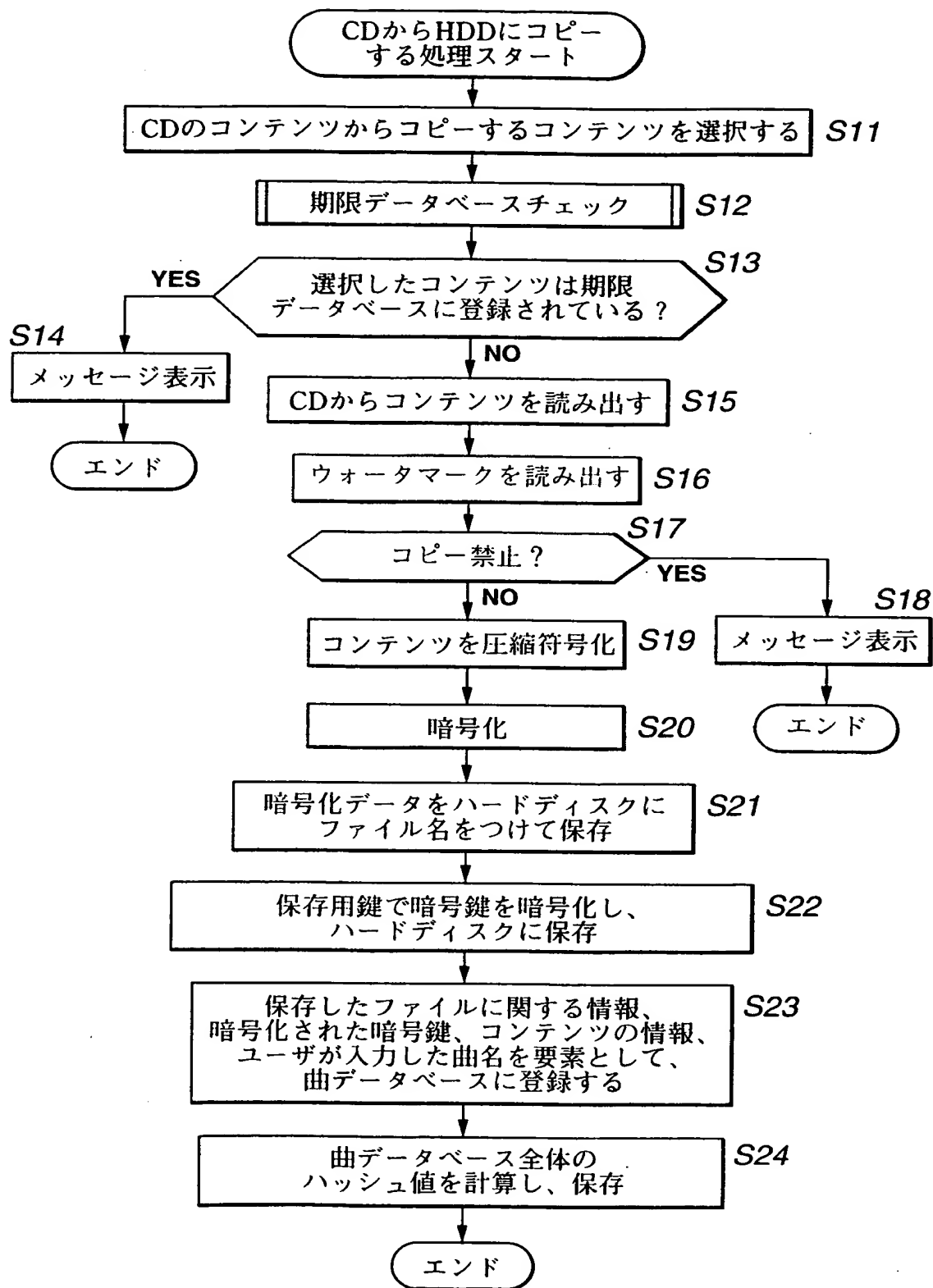


FIG.7

**THIS PAGE BLANK (USPTO)**

8/48

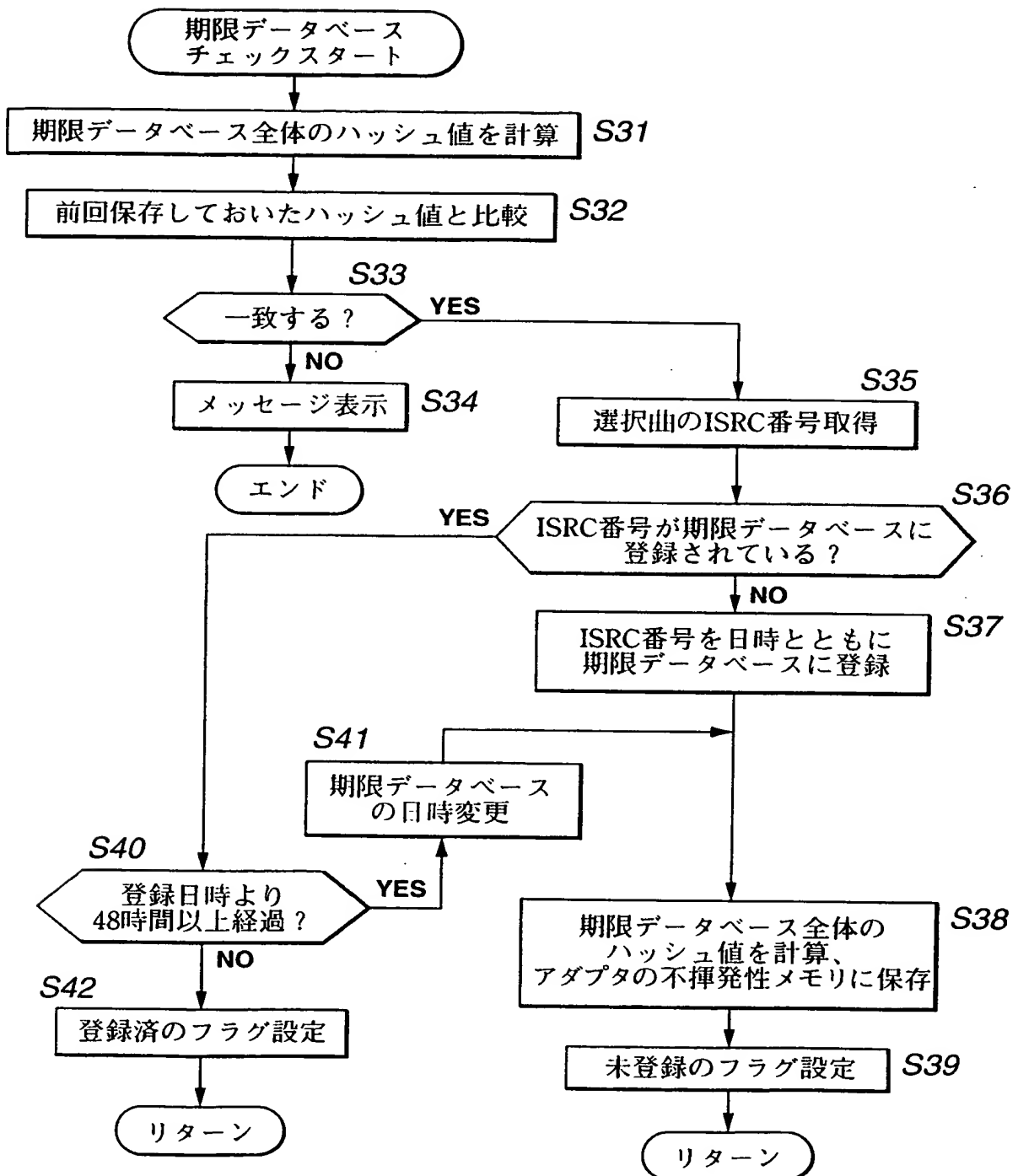


FIG.8

**THIS PAGE BLANK (USPTO)**



	アイテム 1	アイテム 2	アイテム 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934
-------	----------------

FIG.9

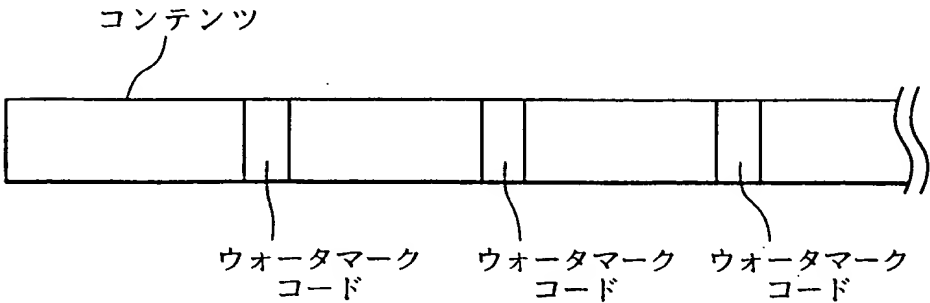


FIG.10

**THIS PAGE BLANK (USPTO)**

	アイテム 1	アイテム 2	アイテム 3	
ファイル名	Xd000110. at2	px92341234. at2	aa0234287034. at2	
暗号化された暗号鍵	0xabababababab	0x98989898989899	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件 : 開始日時	-	2001.01.01.00:00	-	
再生条件 : 終了日時	1999.07.31.23:59	-	-	
再生条件 : 回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	¥ 5	
コピー条件 : 回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件 : SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321
-------	----------------

FIG.11

**THIS PAGE BLANK (USPTO)**

11/48

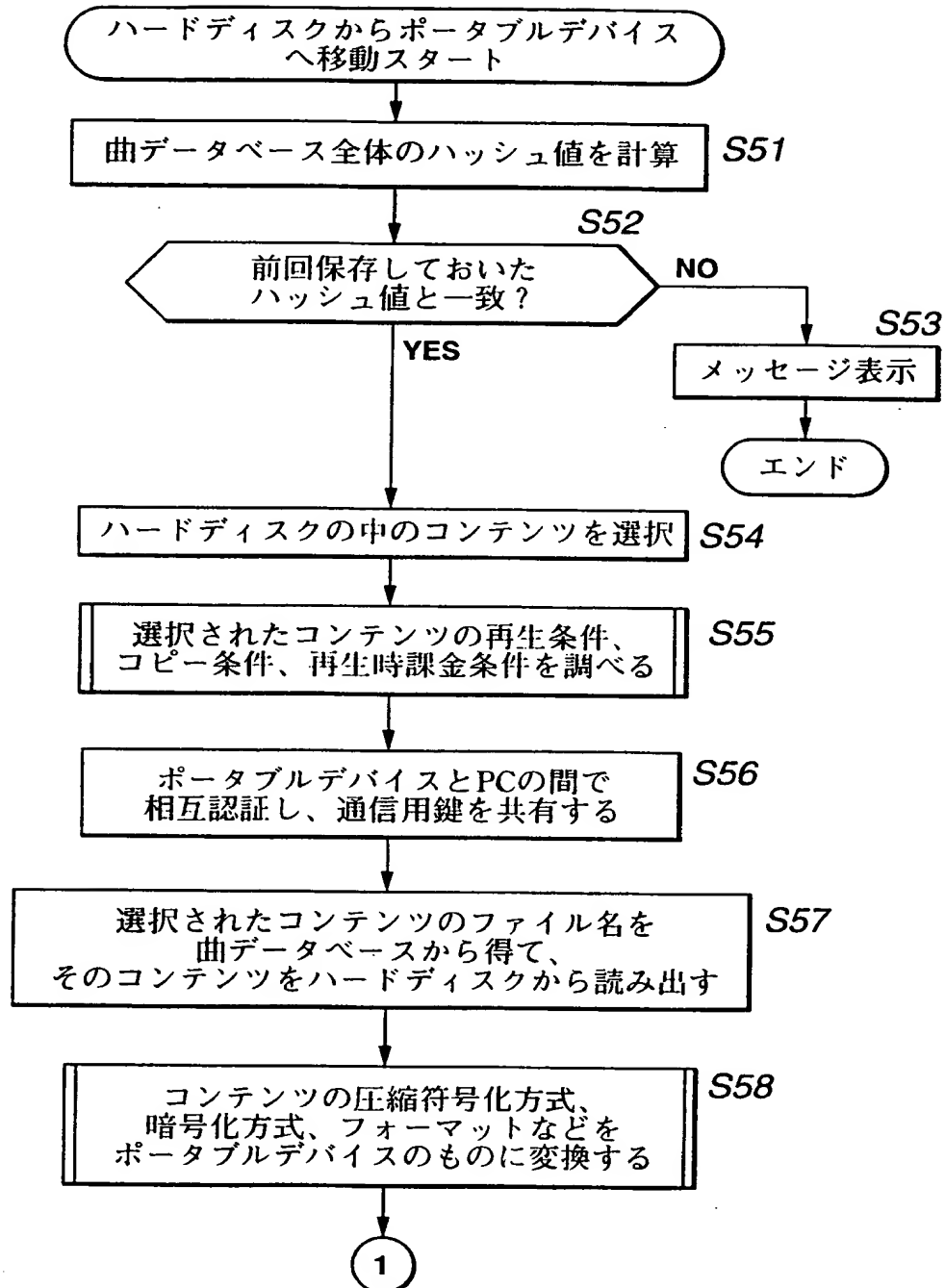


FIG.12

**THIS PAGE BLANK (USPTO)**

12/48

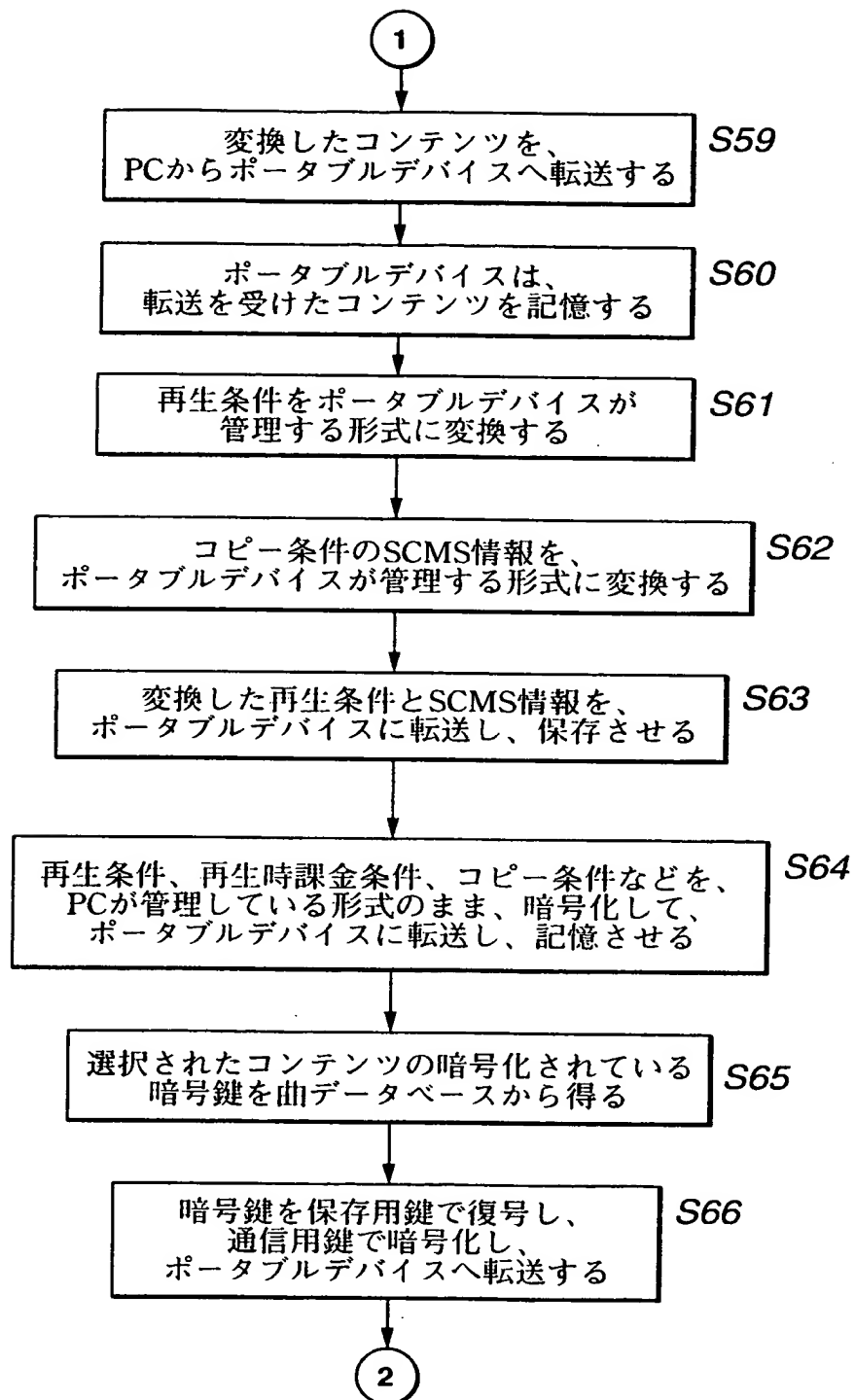


FIG.13

**THIS PAGE BLANK (USPTO)**



13/48

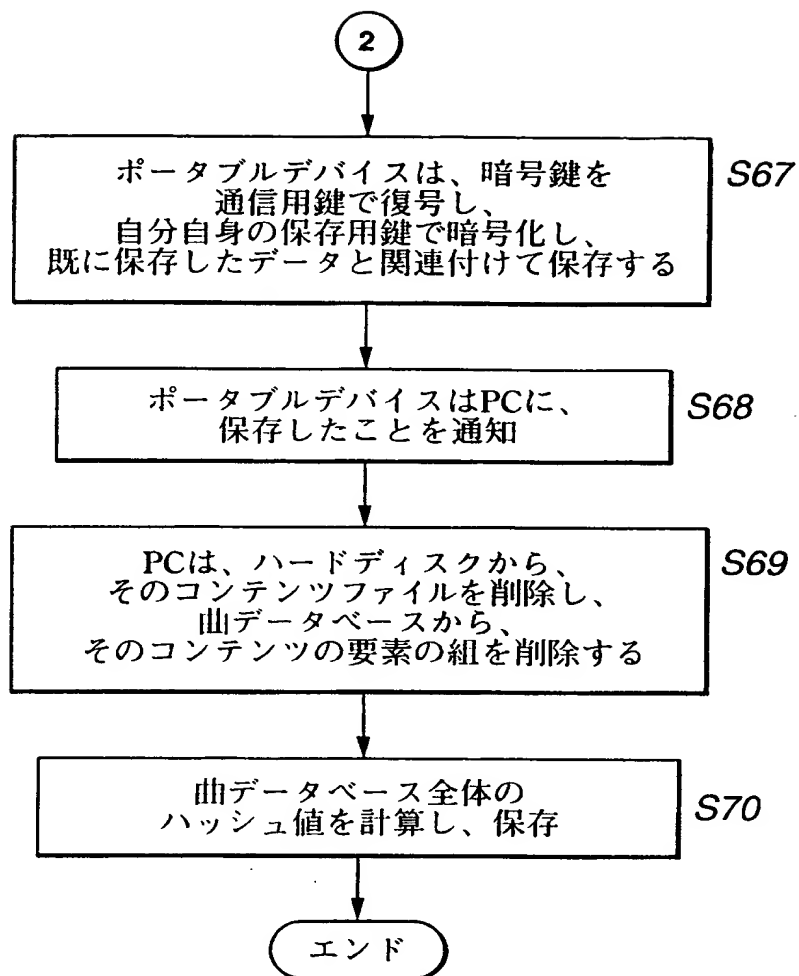


FIG.14

**THIS PAGE BLANK (USPTO)**

14/48

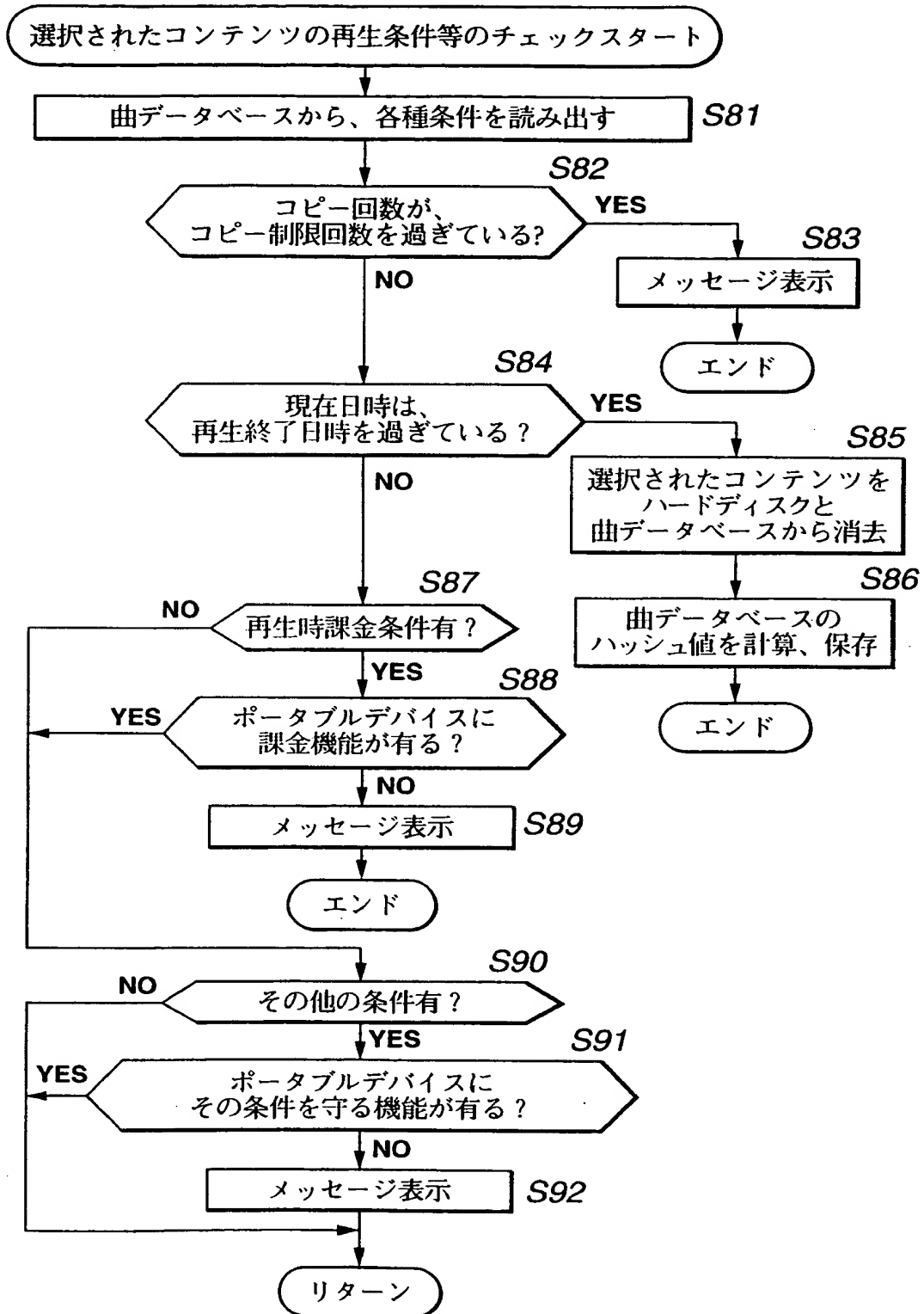


FIG.15

**THIS PAGE BLANK (USPTO)**

	アイテム 1	アイテム 2	アイテム 3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

FIG.16

**THIS PAGE BLANK (USPTO)**

16/48

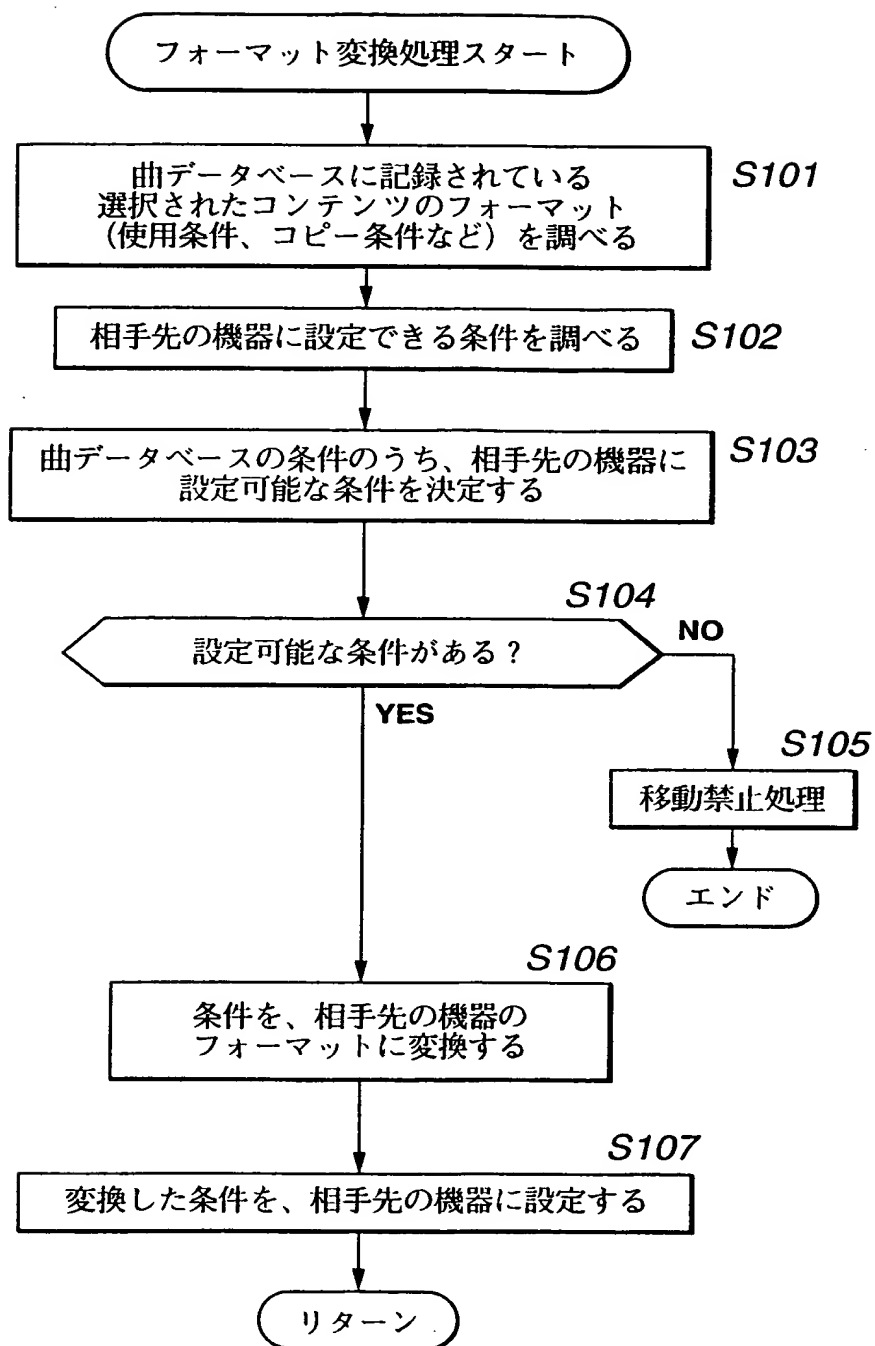


FIG.17

**THIS PAGE BLANK (USPTO)**



17/48

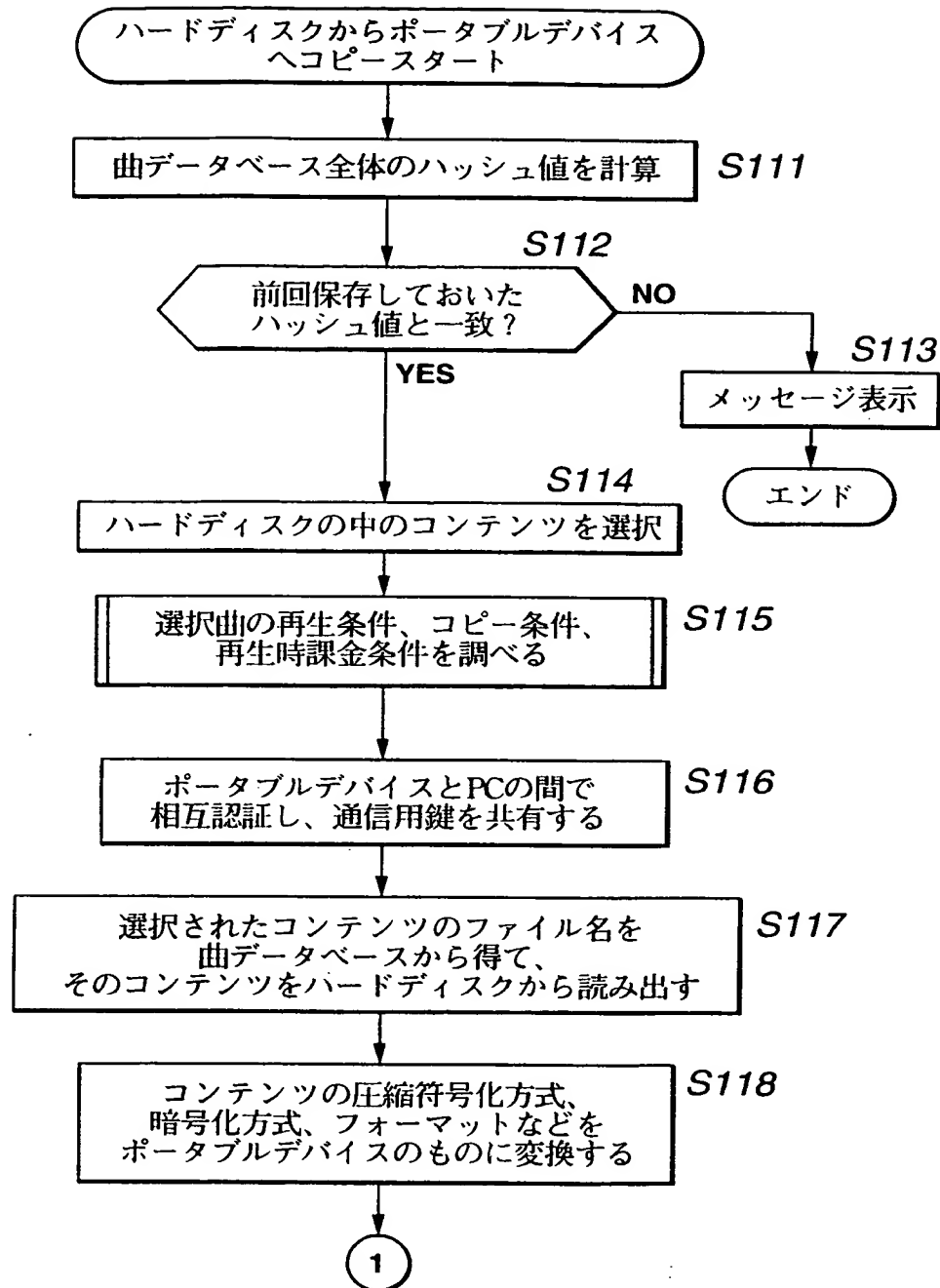


FIG.18

**THIS PAGE BLANK (USPTO)**

18/48

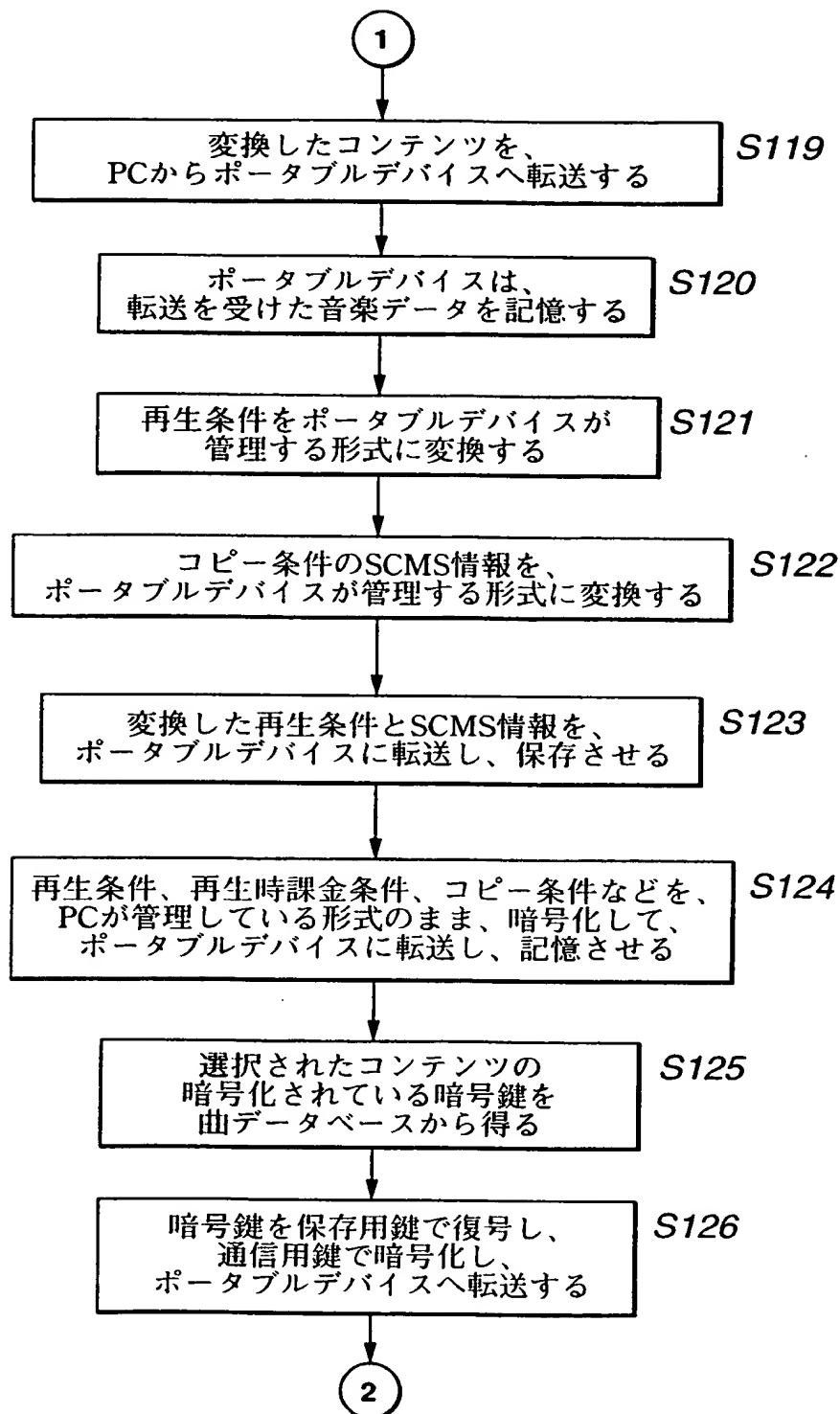


FIG.19

**THIS PAGE BLANK (USPTO)**

19/48

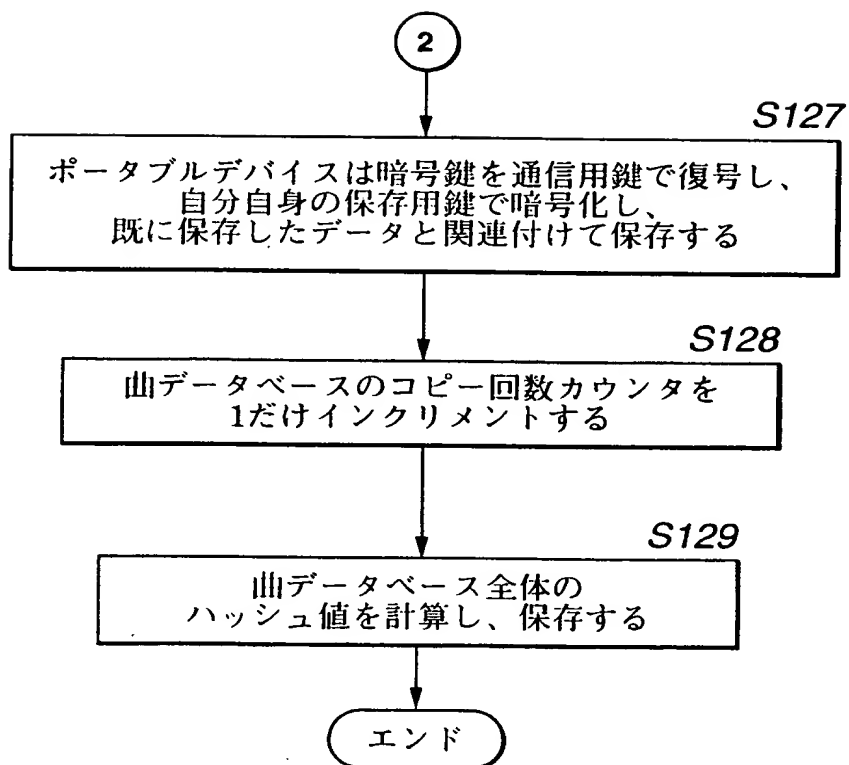


FIG.20

**THIS PAGE BLANK (USPTO)**

20/48

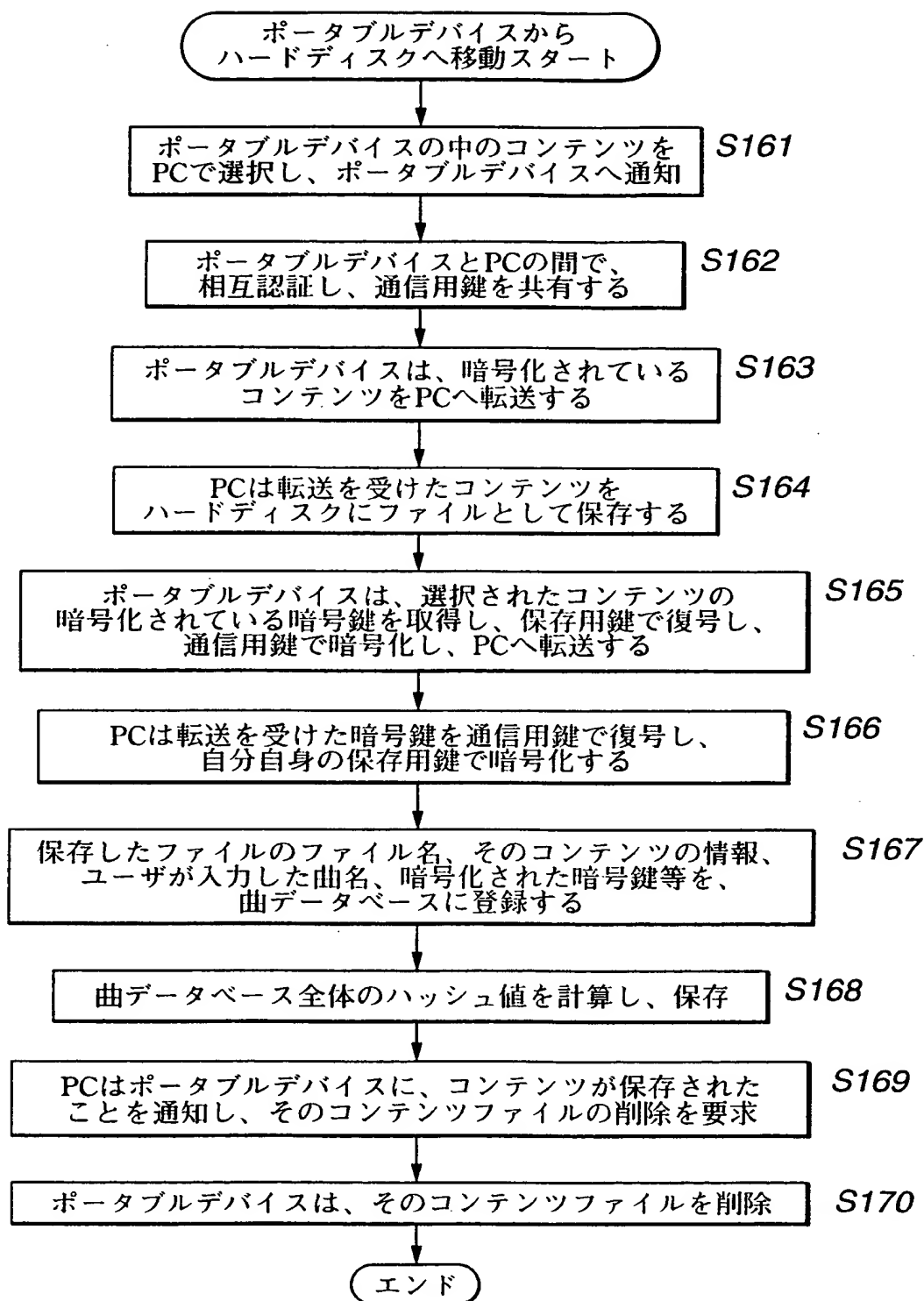


FIG.21

**THIS PAGE BLANK (USPTO)**



21/48

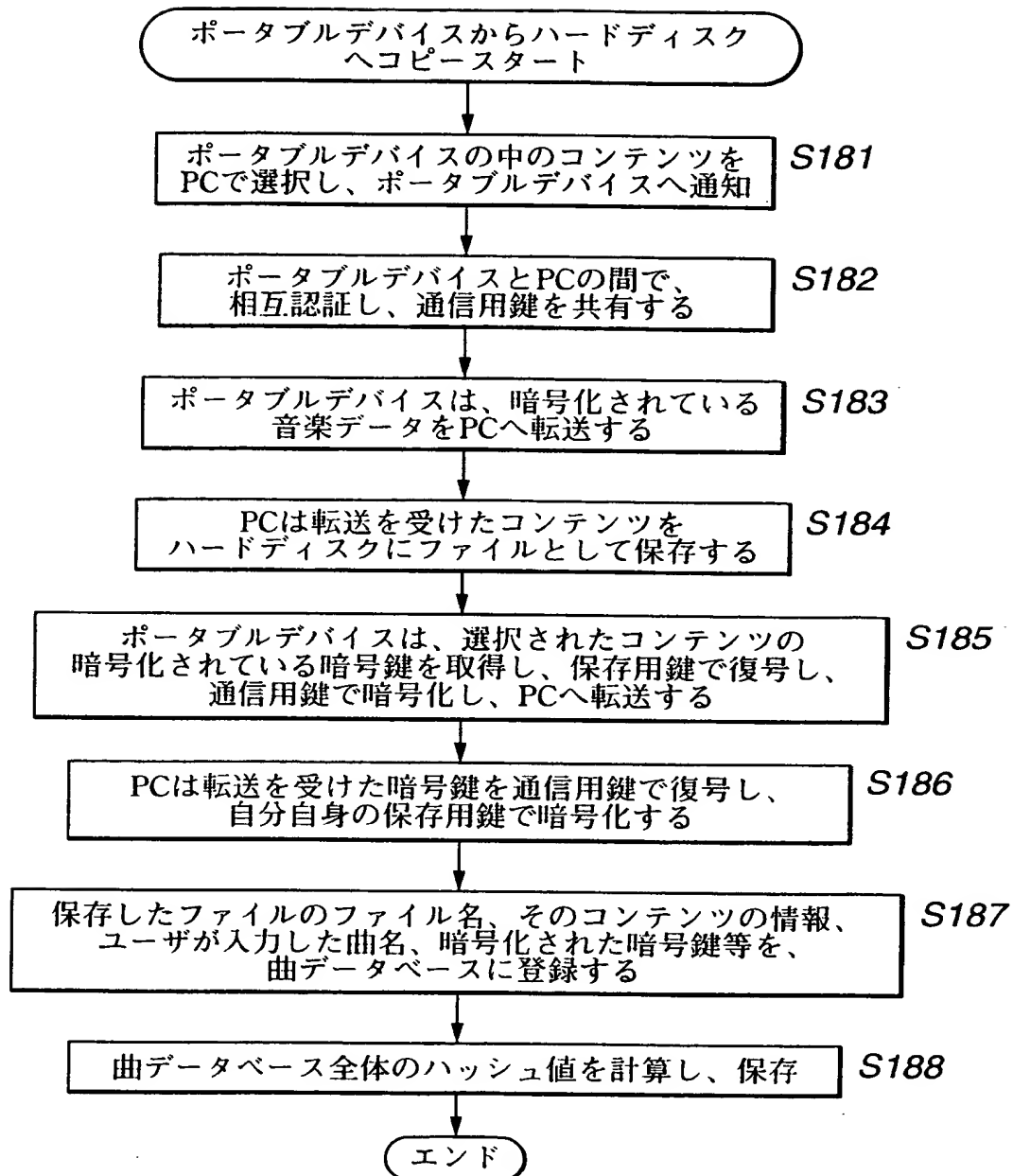


FIG.22

**THIS PAGE BLANK (USPTO)**

22/48



FIG.23

**THIS PAGE BLANK (USPTO)**

23/48

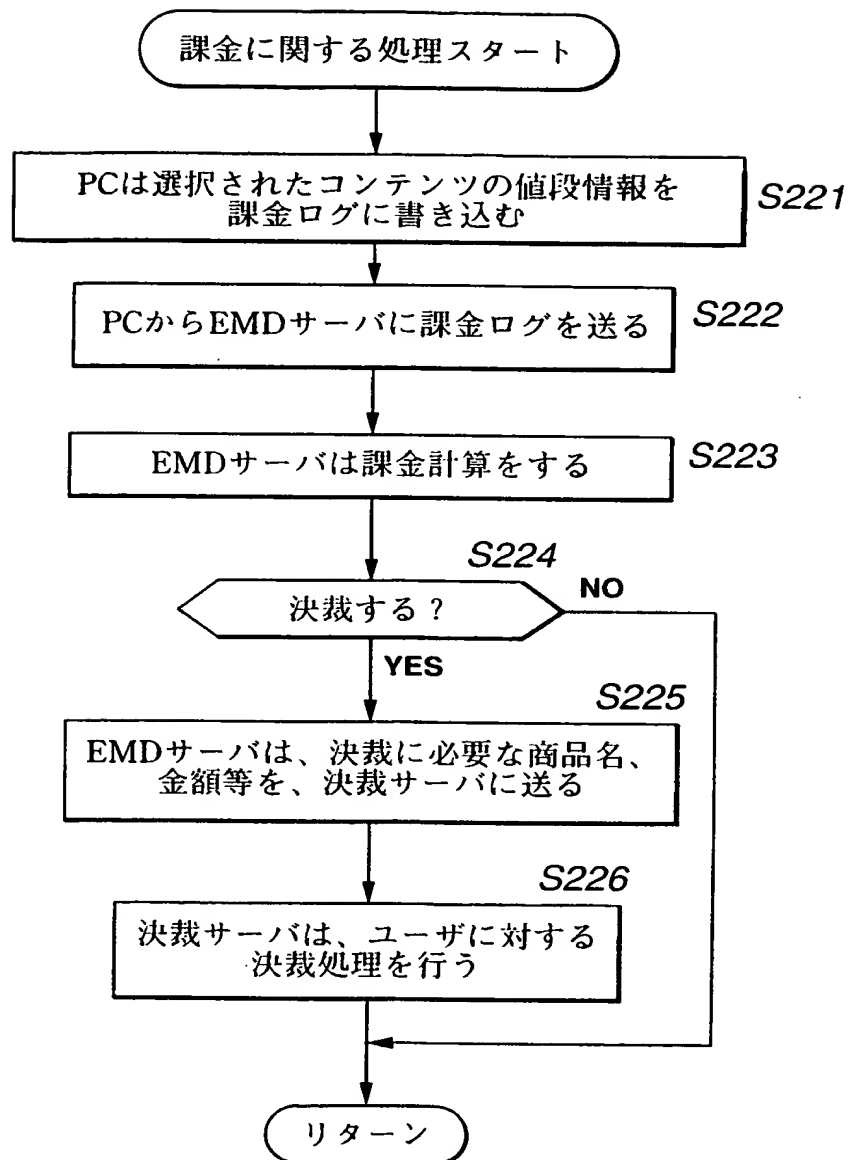


FIG.24

**THIS PAGE BLANK (USPTO)**

	アイテム 1	アイテム 2	アイテム 3	
料金	50	50	60	

ハッシュ値	0xf8783e263517
-------	----------------

FIG.25

**THIS PAGE BLANK (USPTO)**



25/48

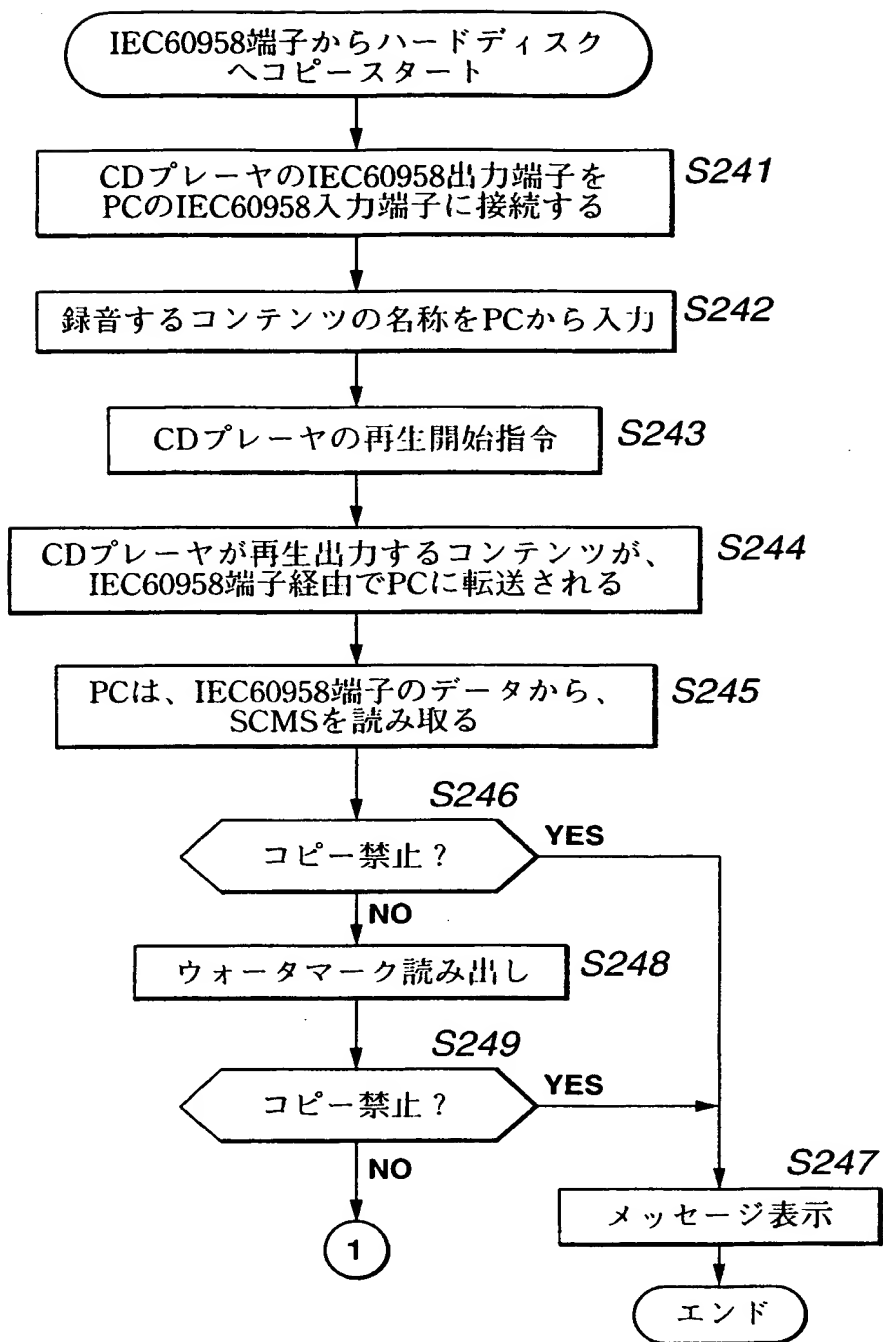


FIG.26

**THIS PAGE BLANK (USPTO)**

26/48

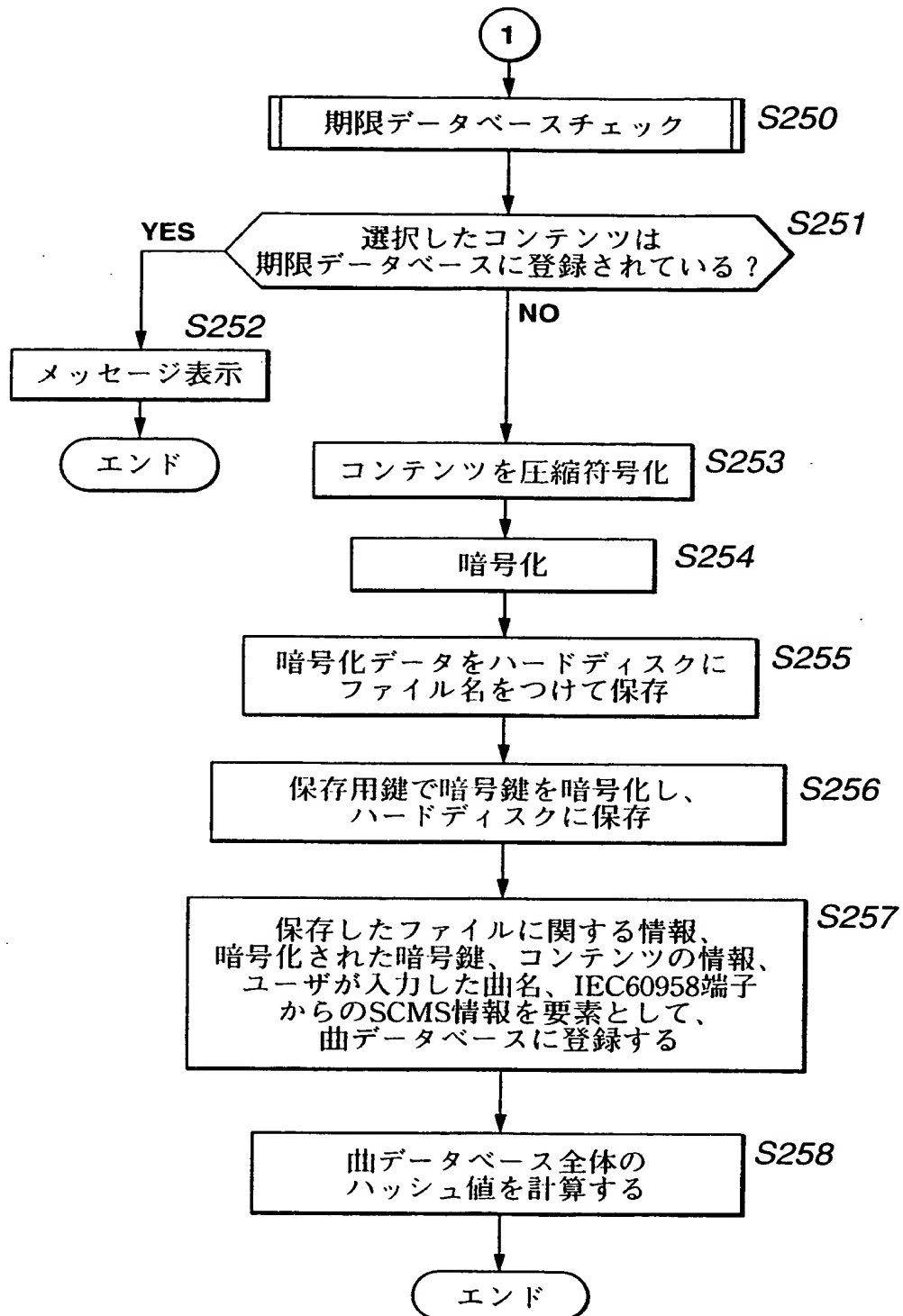


FIG.27

**THIS PAGE BLANK (USPTO)**

27/48

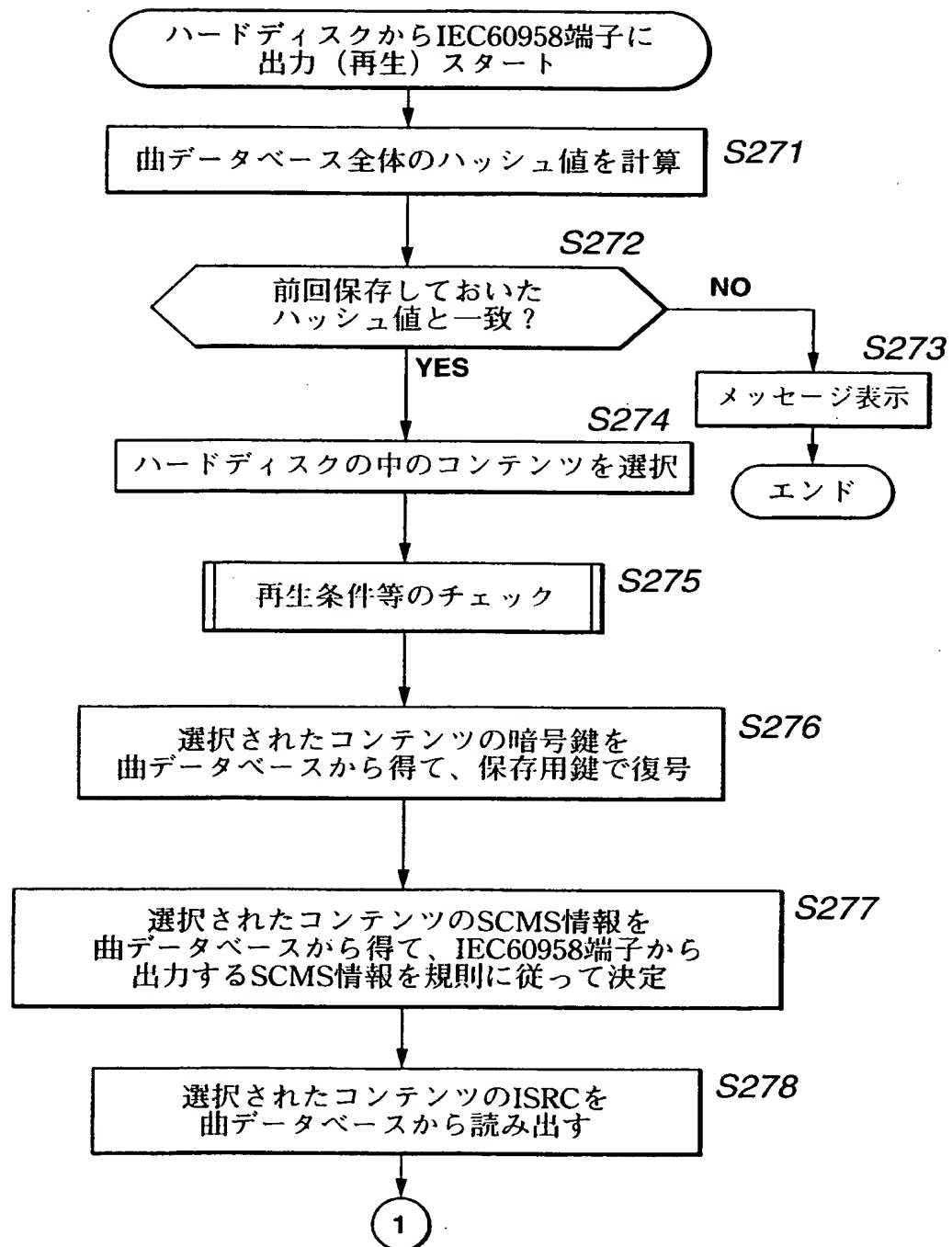


FIG.28

**PAGE BLANK (USPTO)**

28/48

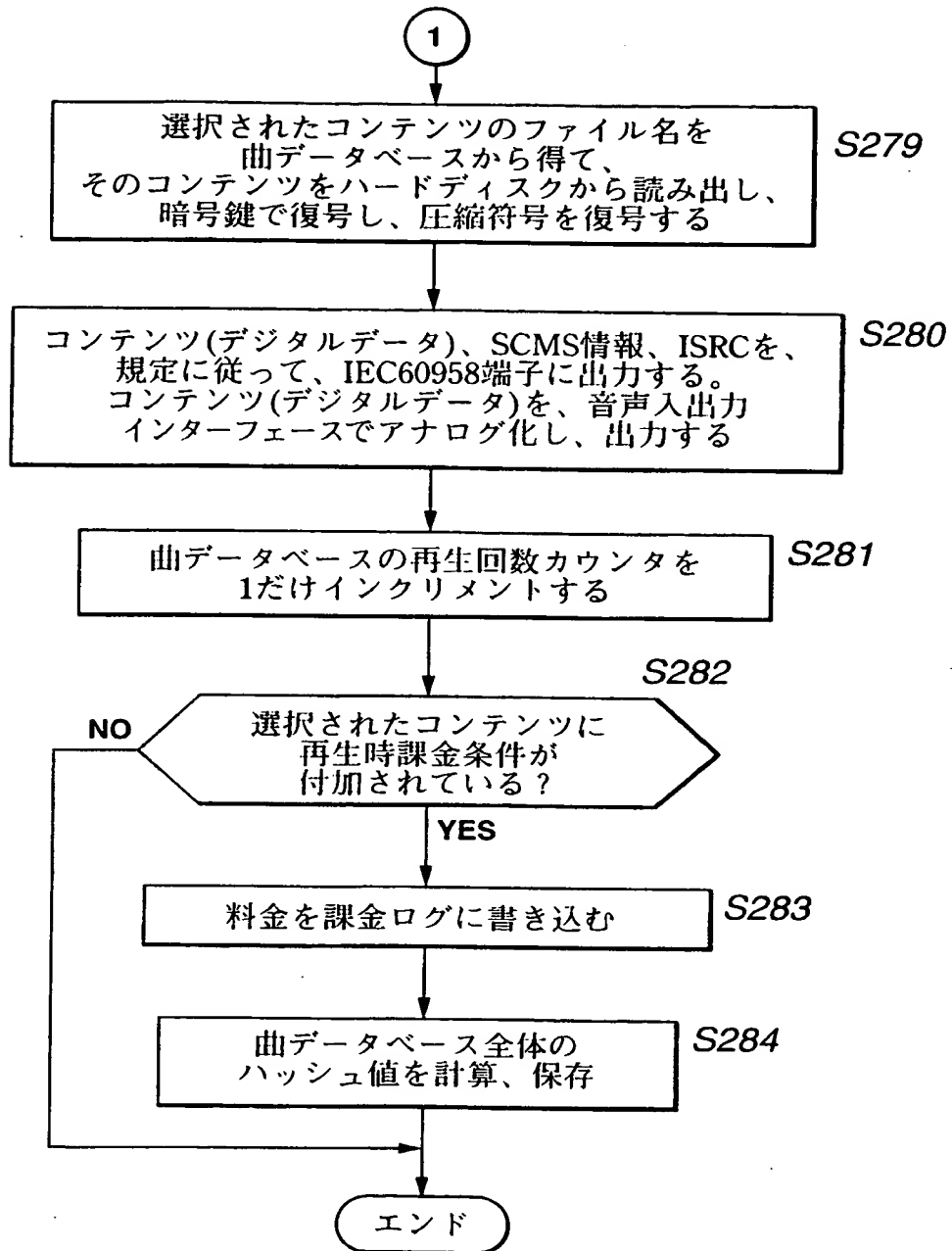


FIG.29

**THIS PAGE BLANK (USPTO)**



29/48

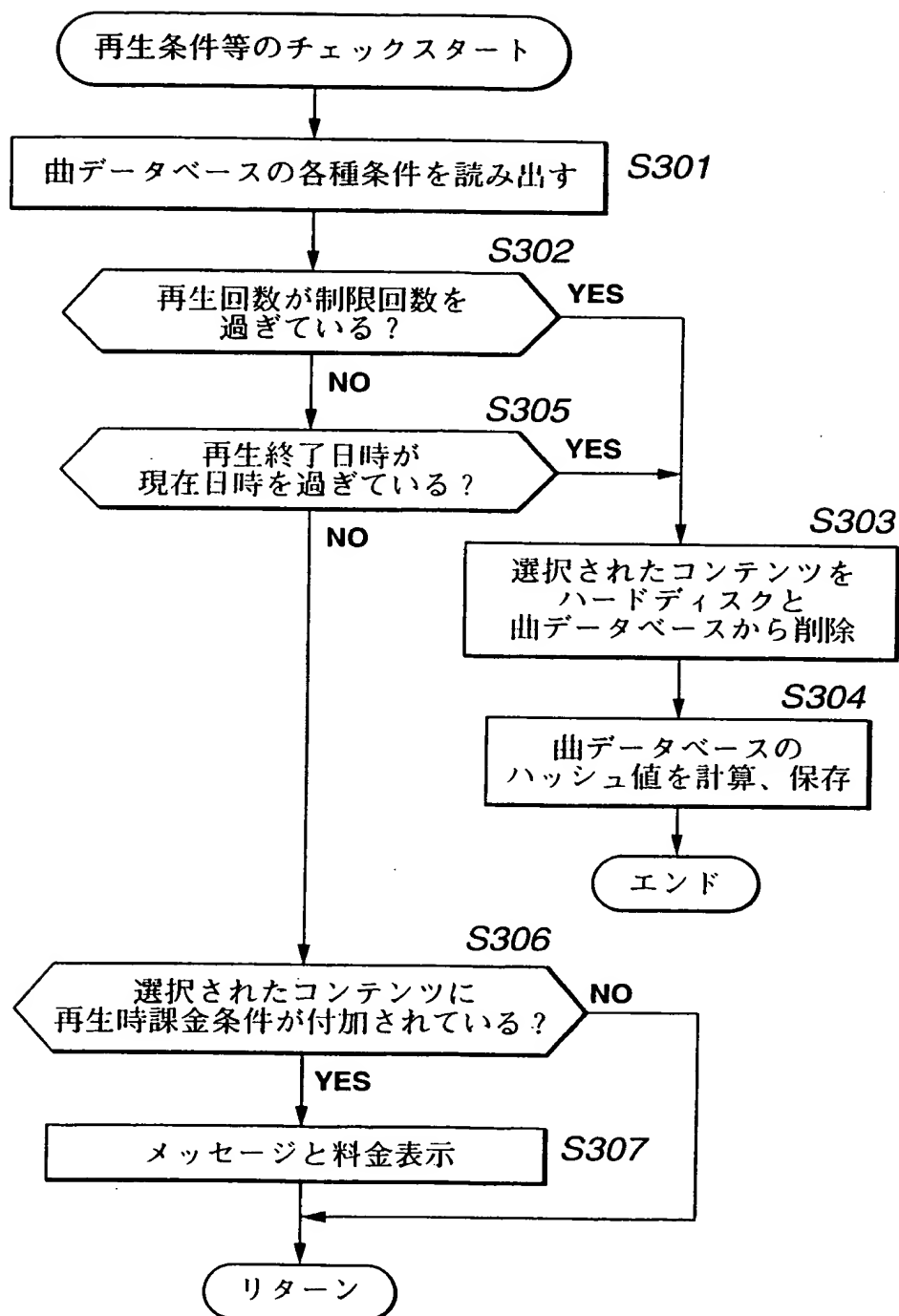


FIG.30

**THIS PAGE BLANK (USPTO)**

30/48

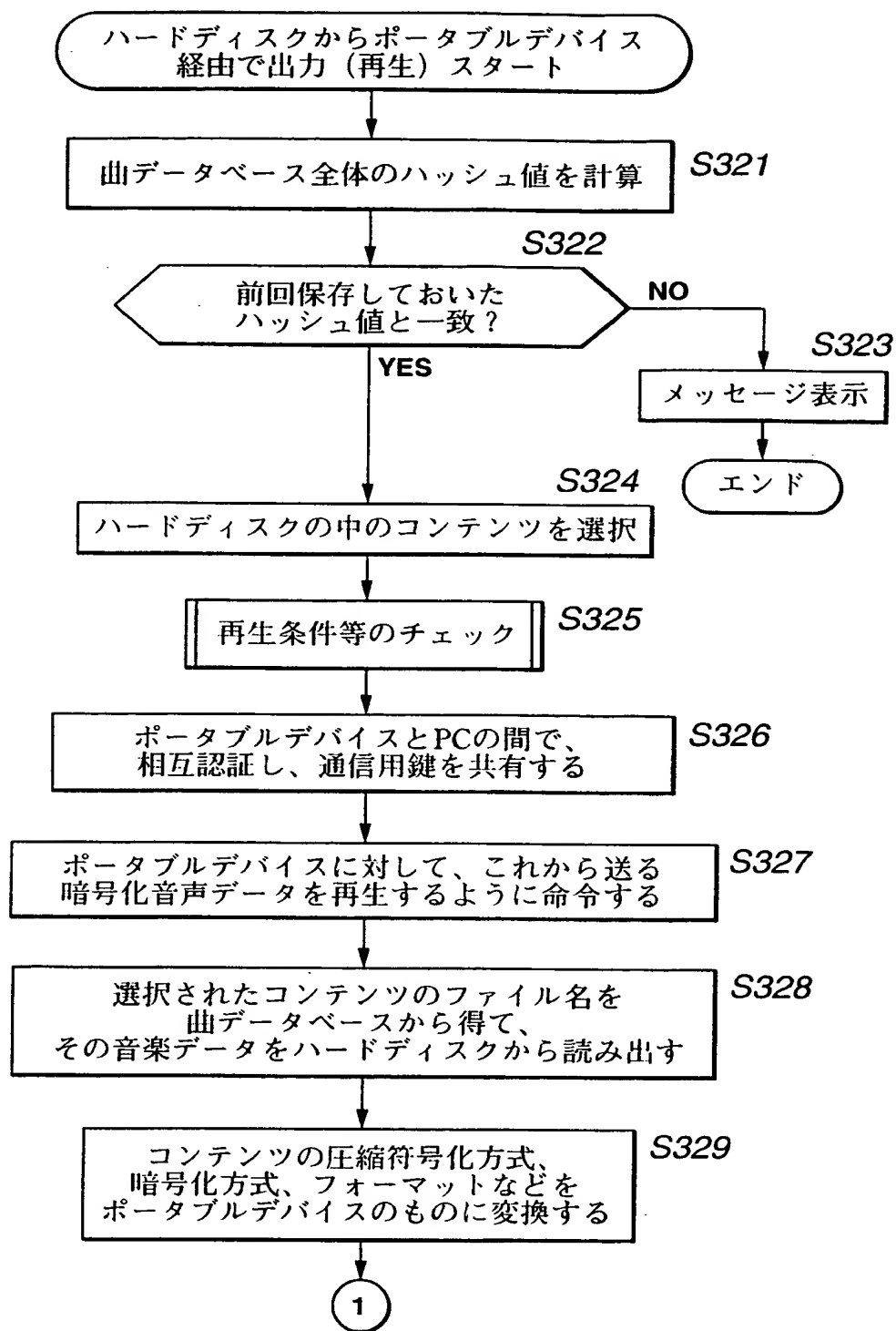


FIG.31

**THIS PAGE BLANK (USPTO)**

31/48

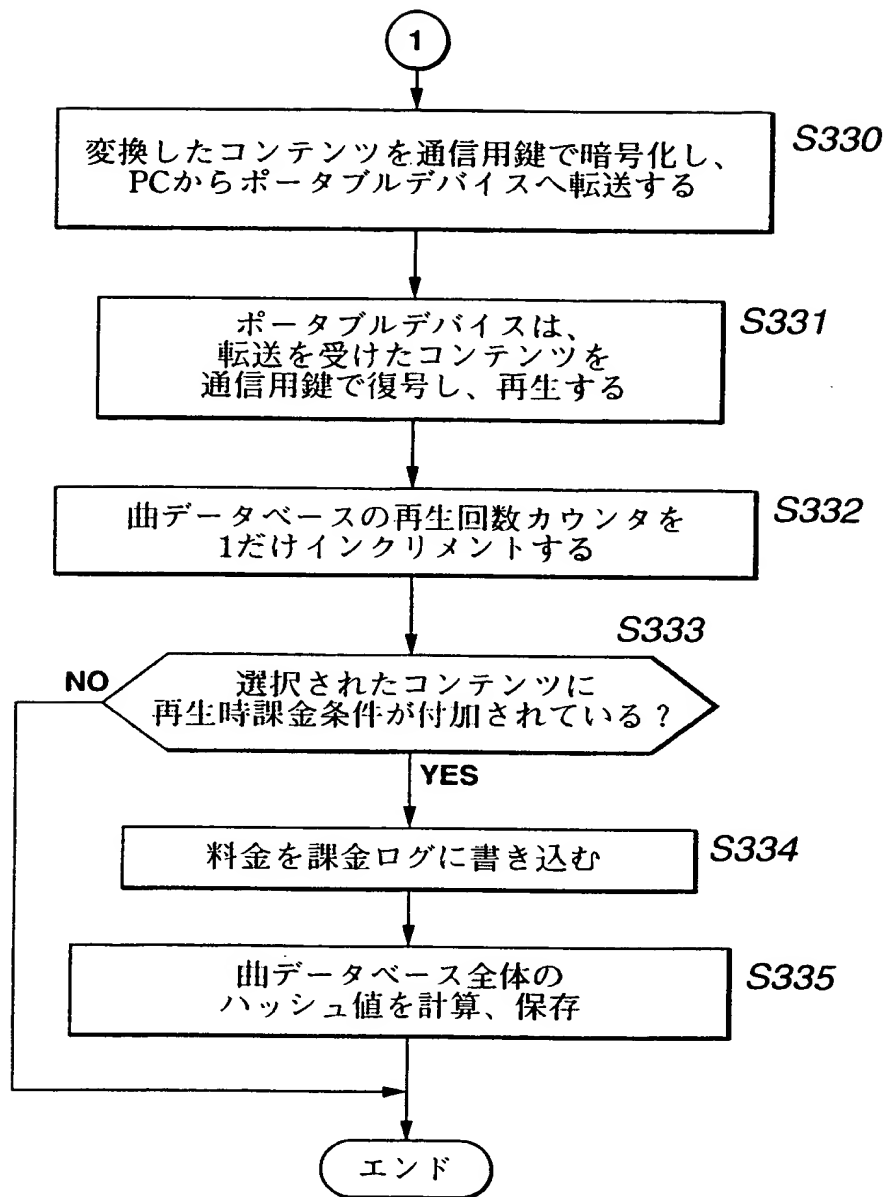


FIG.32

**THIS PAGE BLANK (USPTO)**

32/48

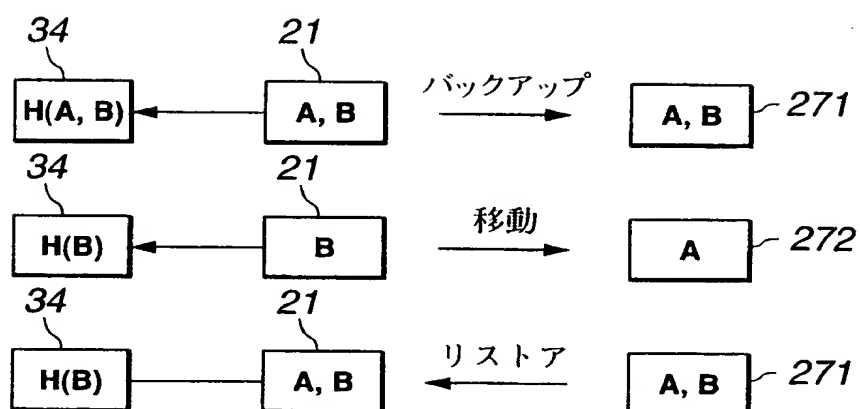


FIG.33

**THIS PAGE BLANK (USPTO)**



33/48

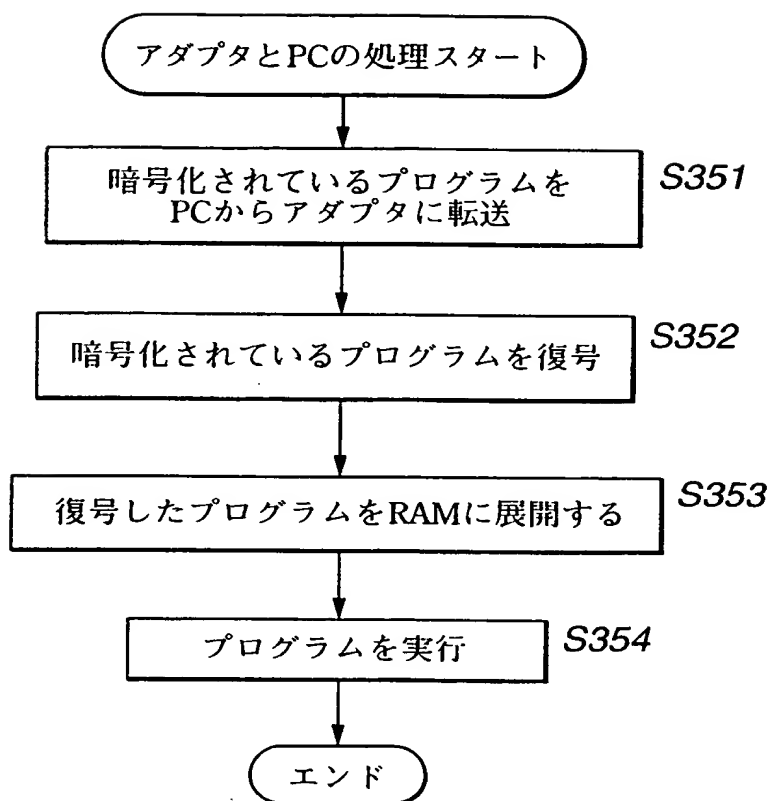
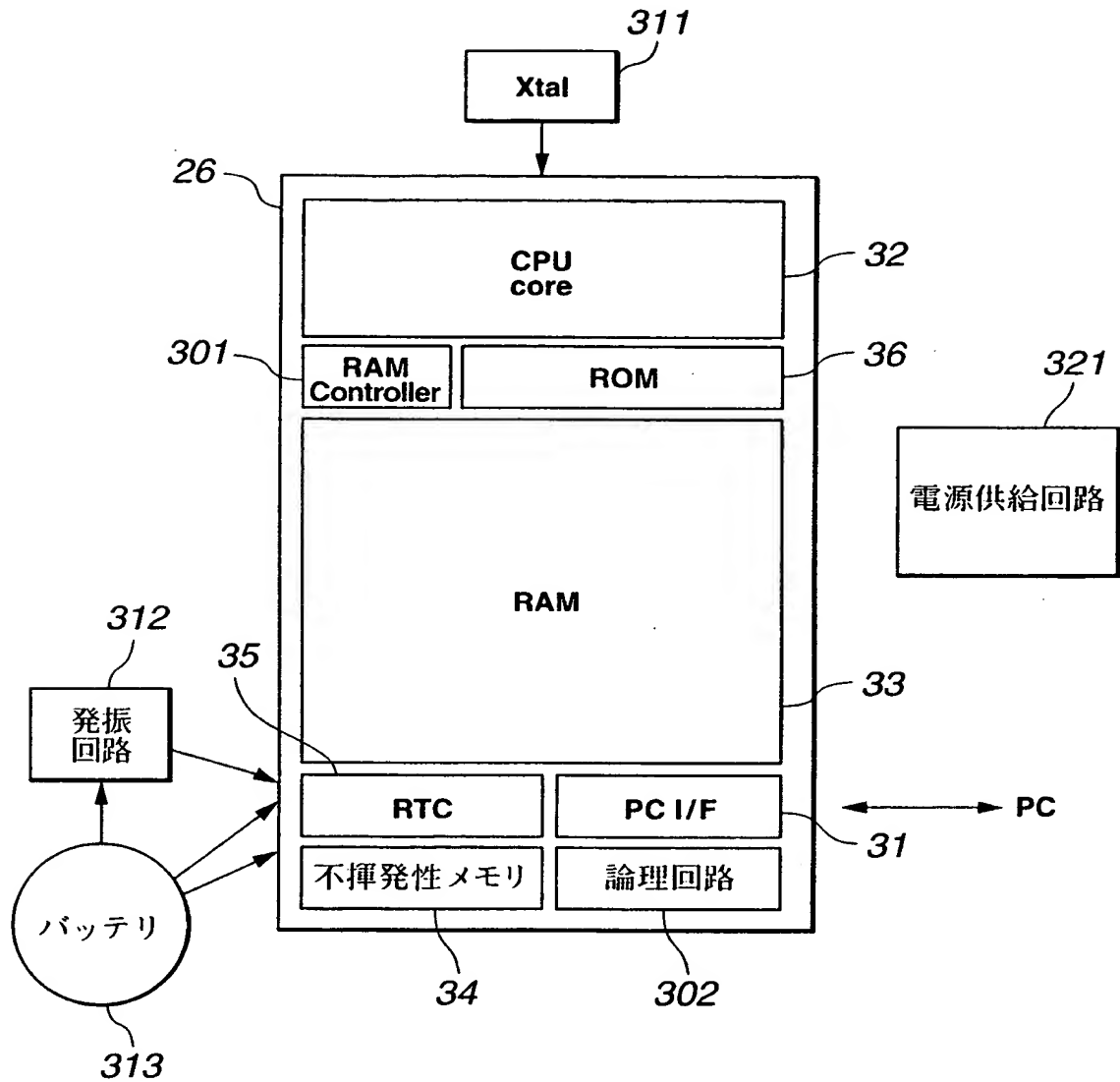


FIG.34

**THIS PAGE BLANK (USPTO)**

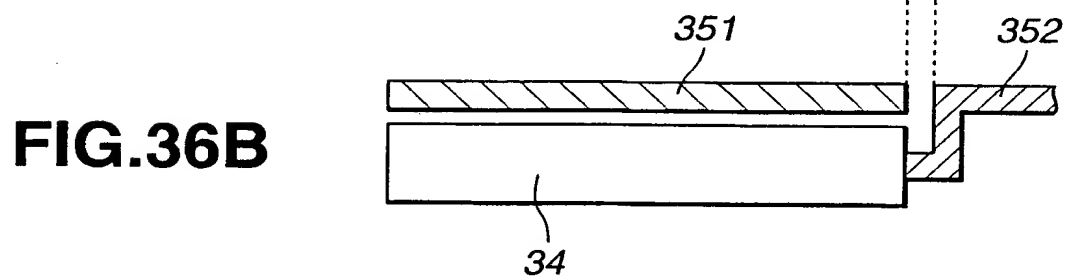
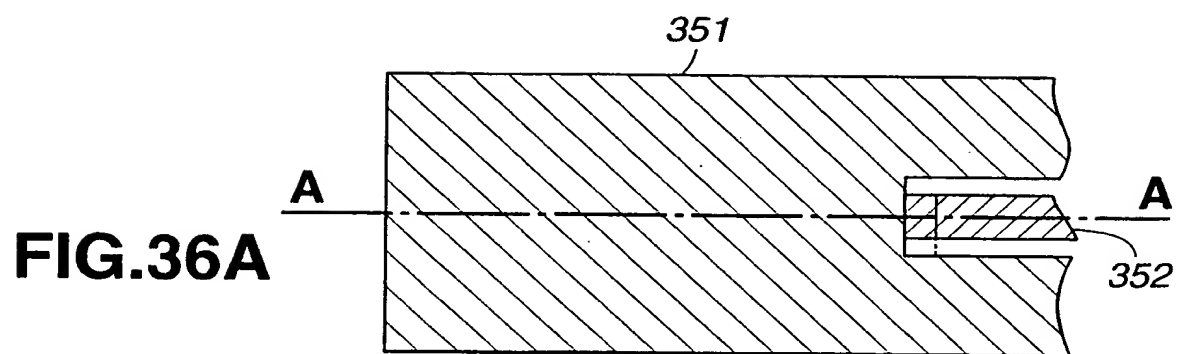
**34/48**



**FIG.35**

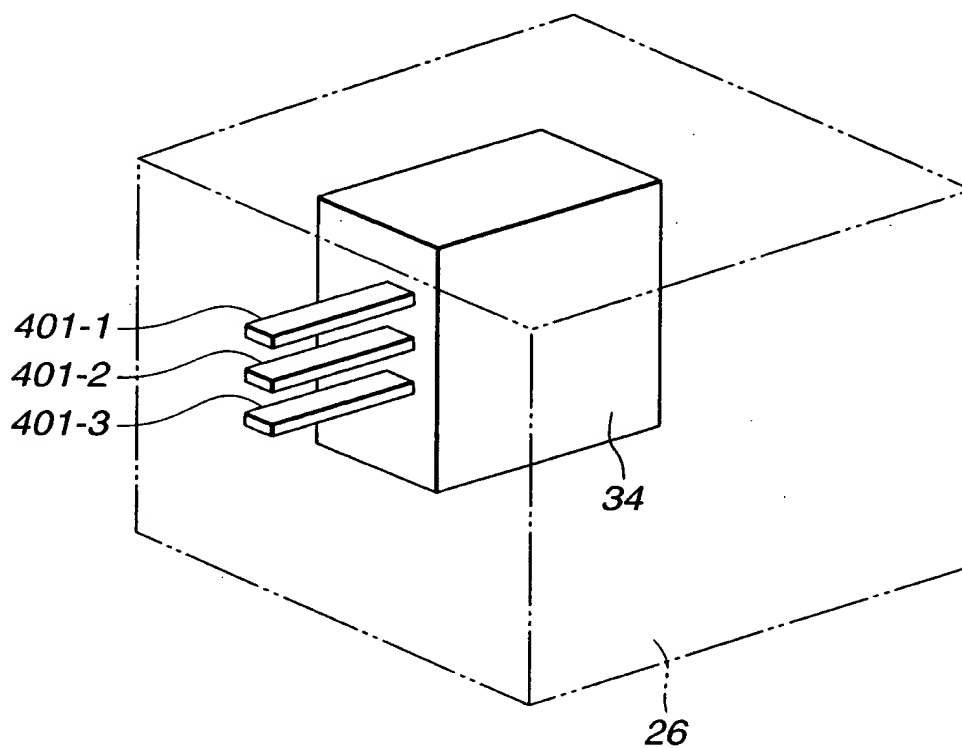
**THIS PAGE BLANK (USPTO)**

35/48



**THIS PAGE BLANK (USPTO)**

36/48



**FIG.37**

**THIS PAGE BLANK (USPTO)**



37/ 48

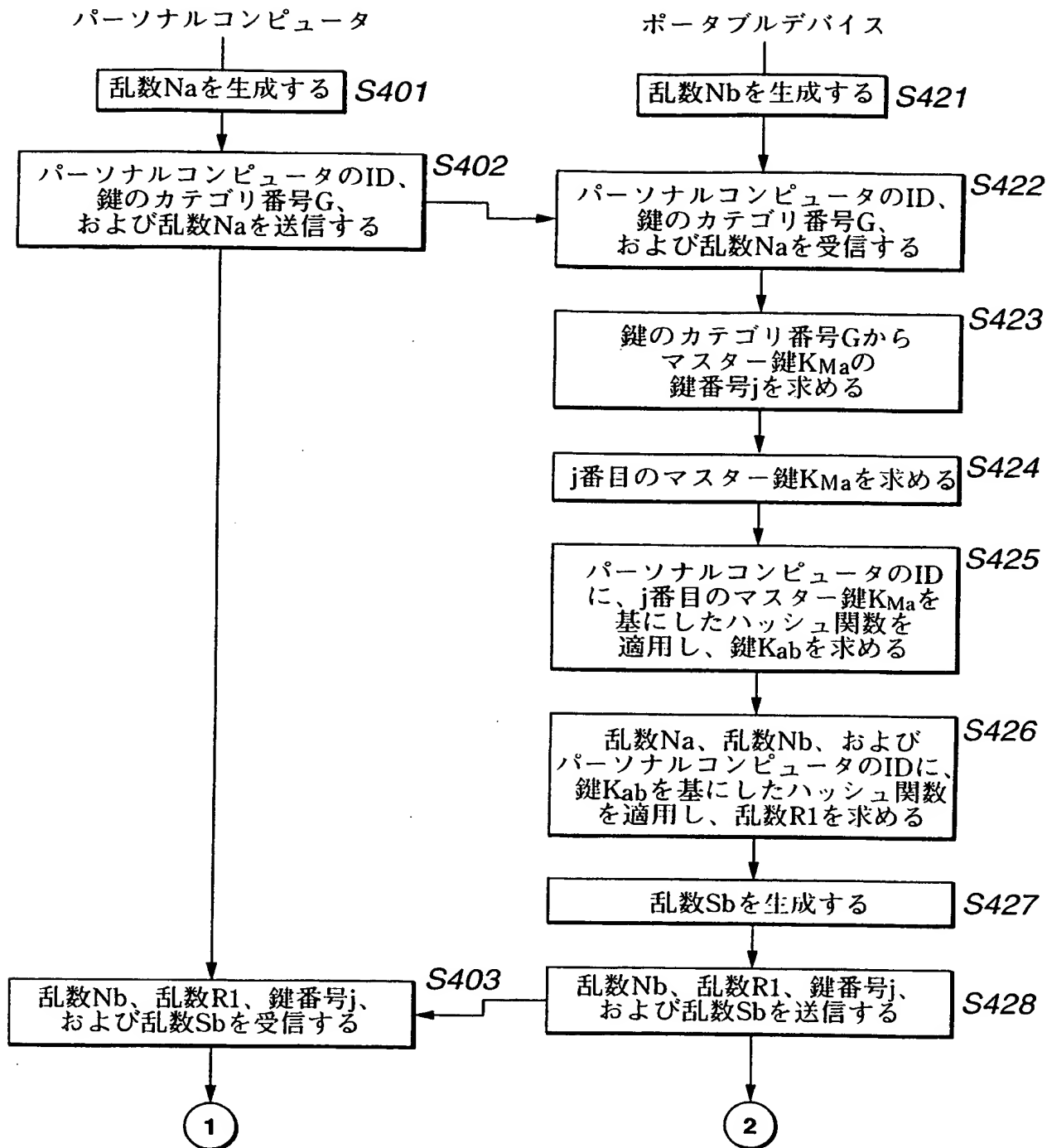


FIG.38

**THIS PAGE BLANK (USPTO)**

38/48

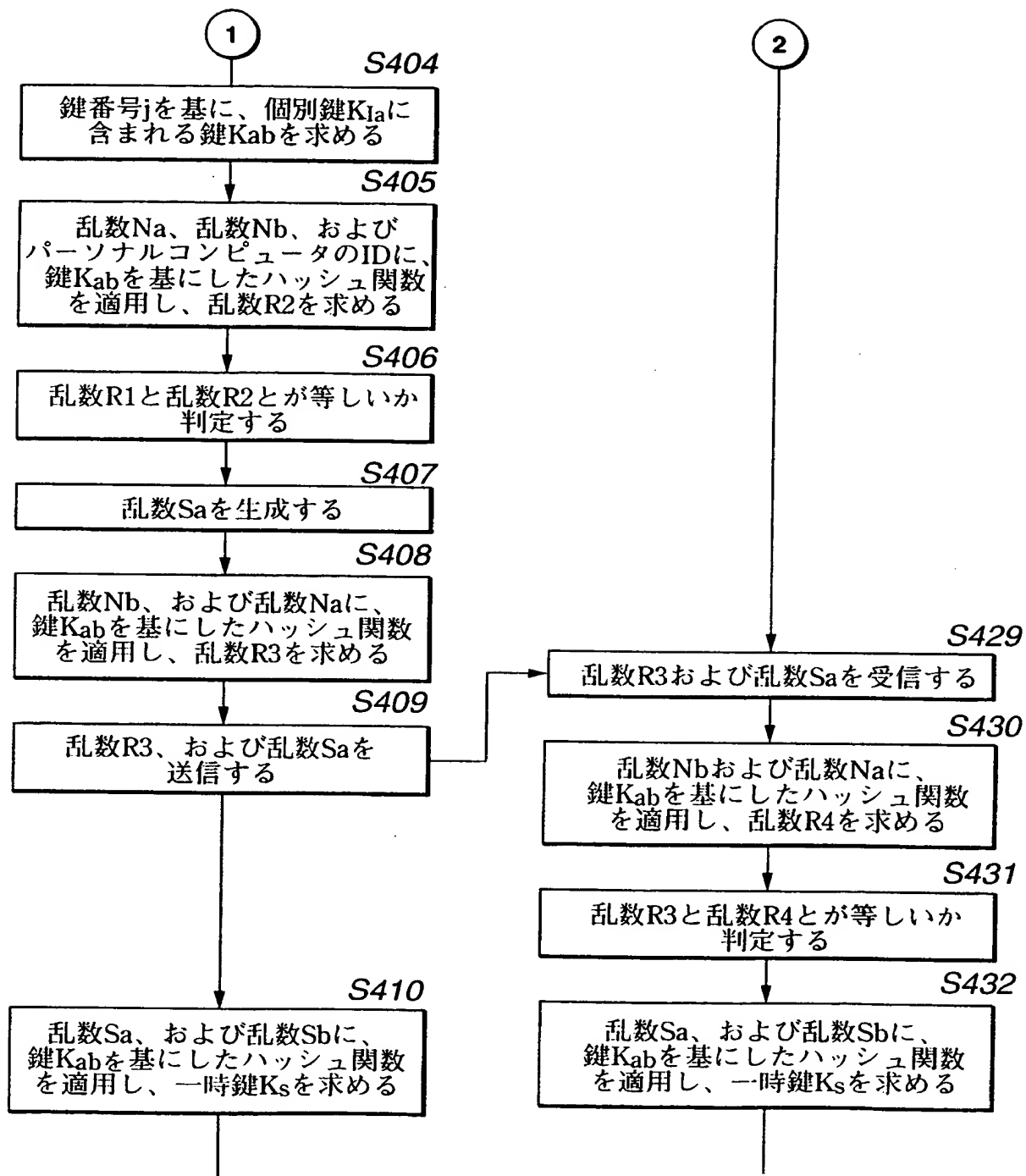


FIG.39

**THIS PAGE BLANK (USPTO)**

39/48

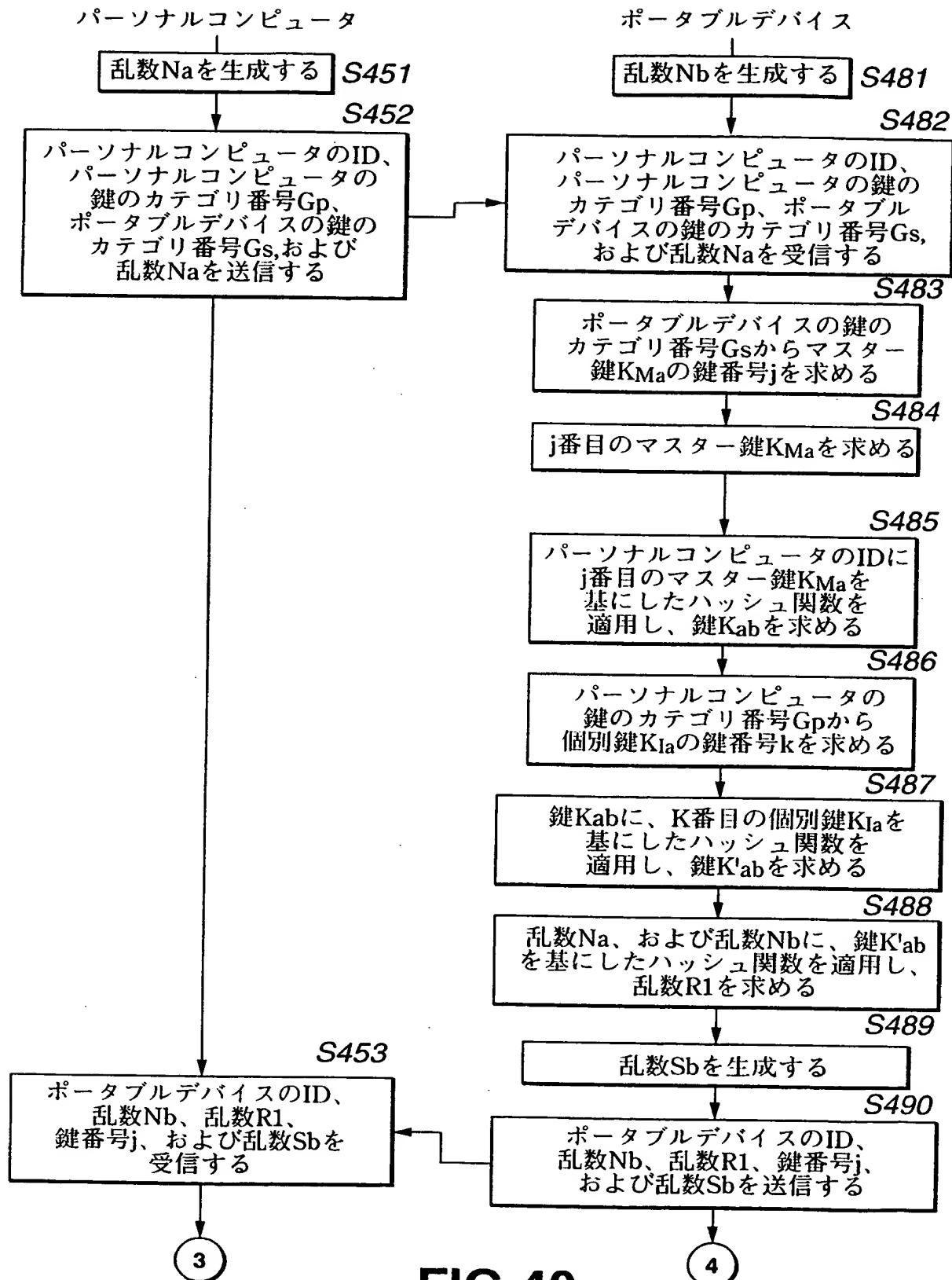


FIG.40

**THIS PAGE BLANK (USPTO)**

40/48

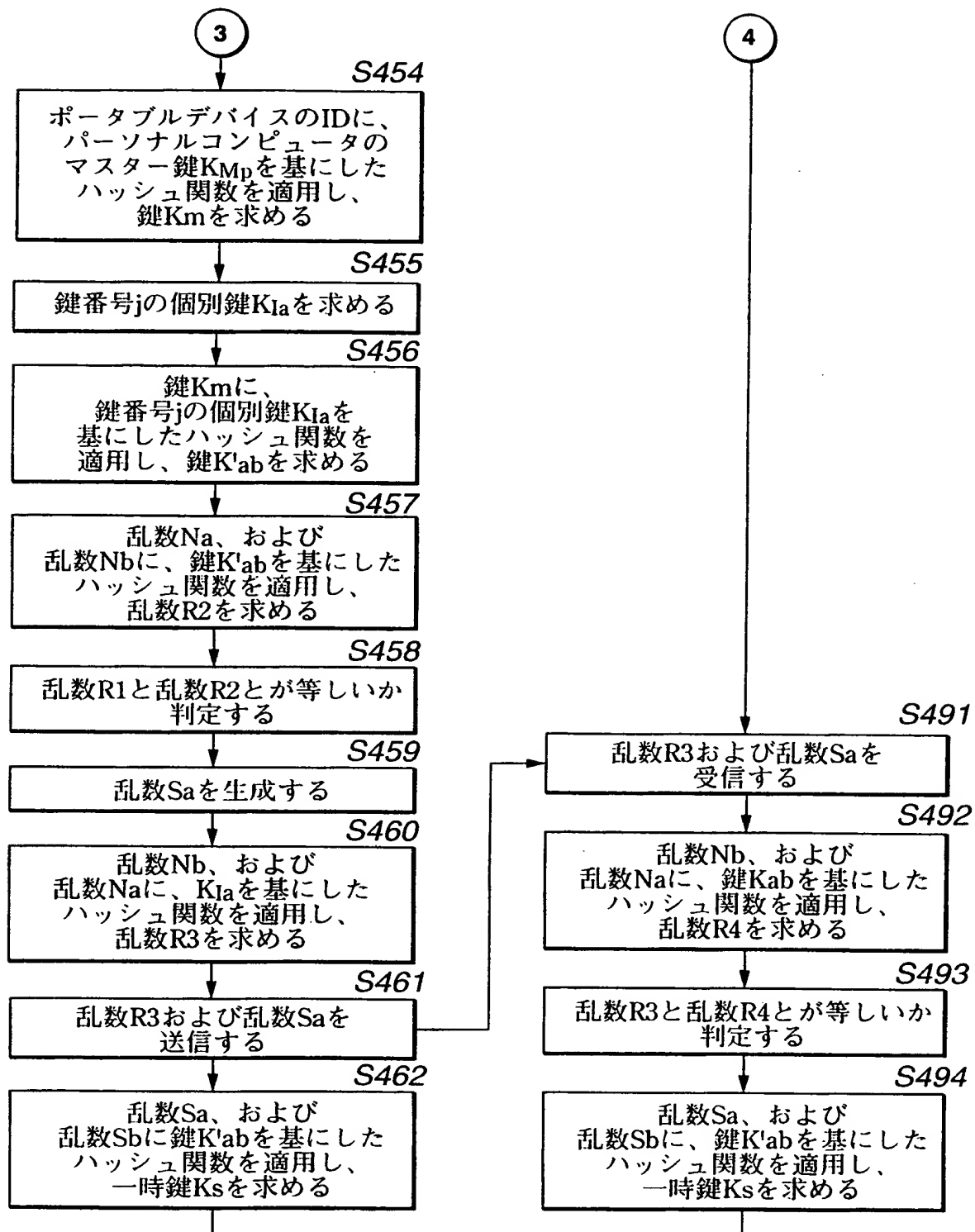


FIG. 41

**THIS PAGE BLANK (USPTO)**



41/48

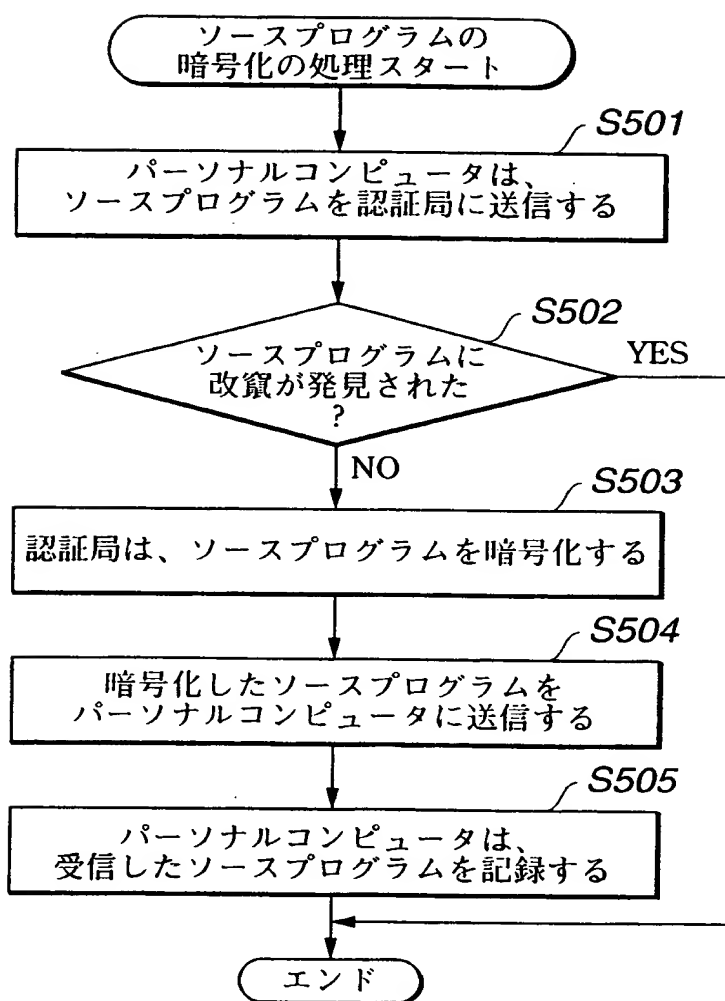


FIG.42

**THIS PAGE BLANK (USPTO)**

42/48

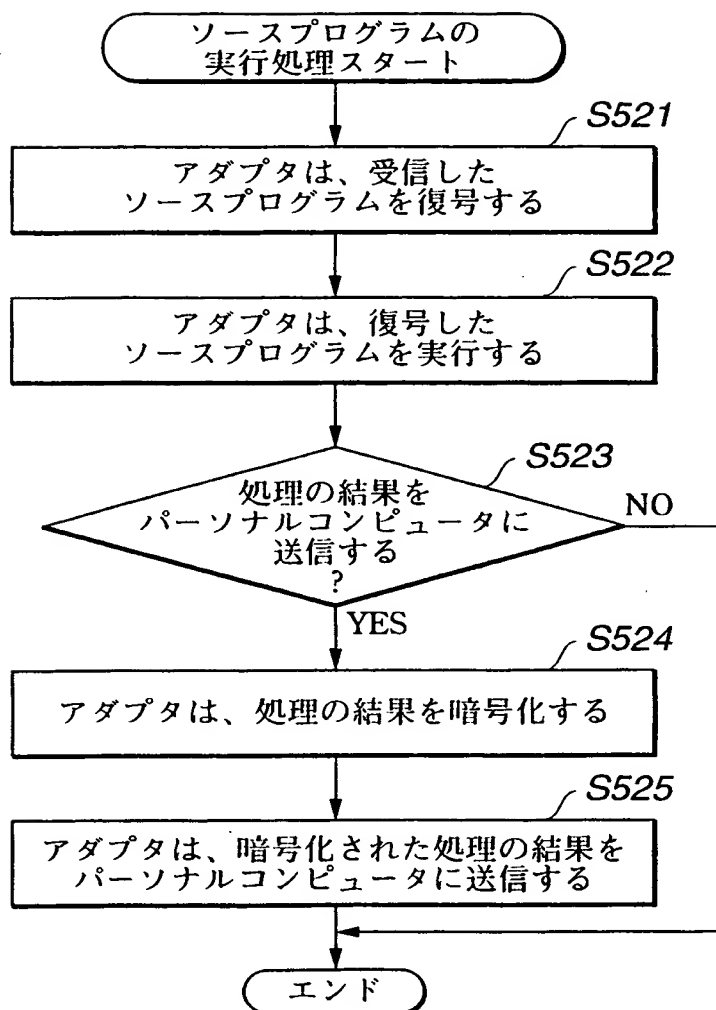


FIG.43

**THIS PAGE BLANK (USPTO)**

43/48

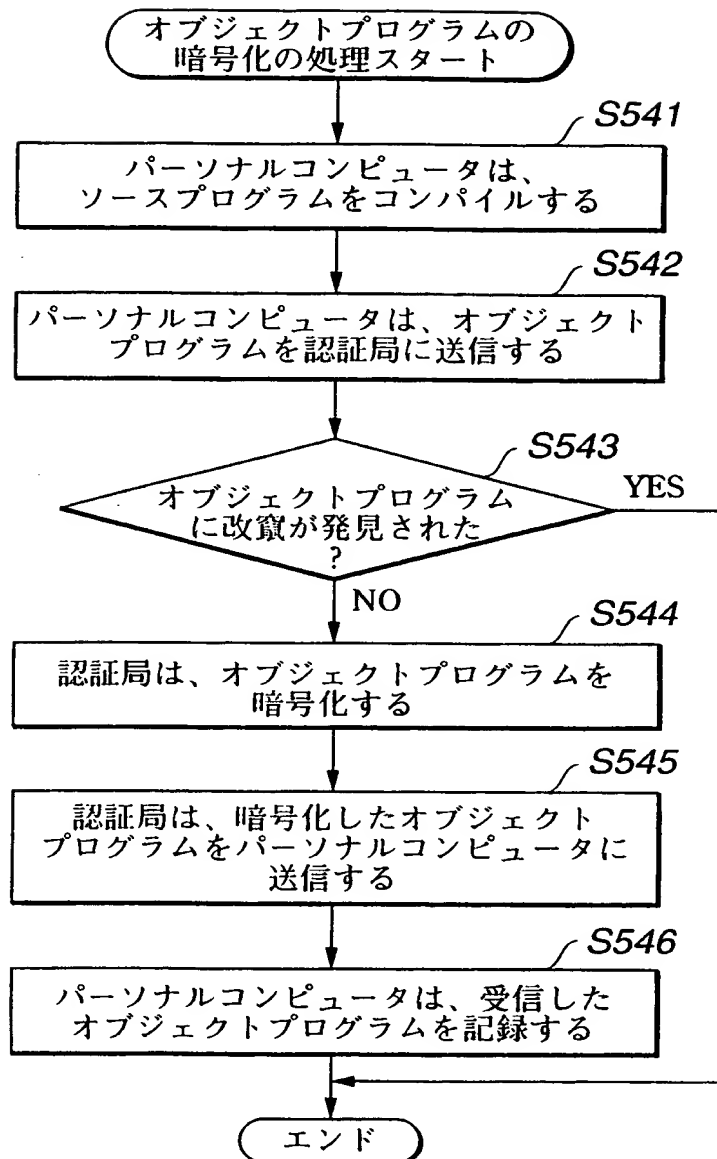


FIG.44

**THIS PAGE BLANK (USPTO)**

44/48

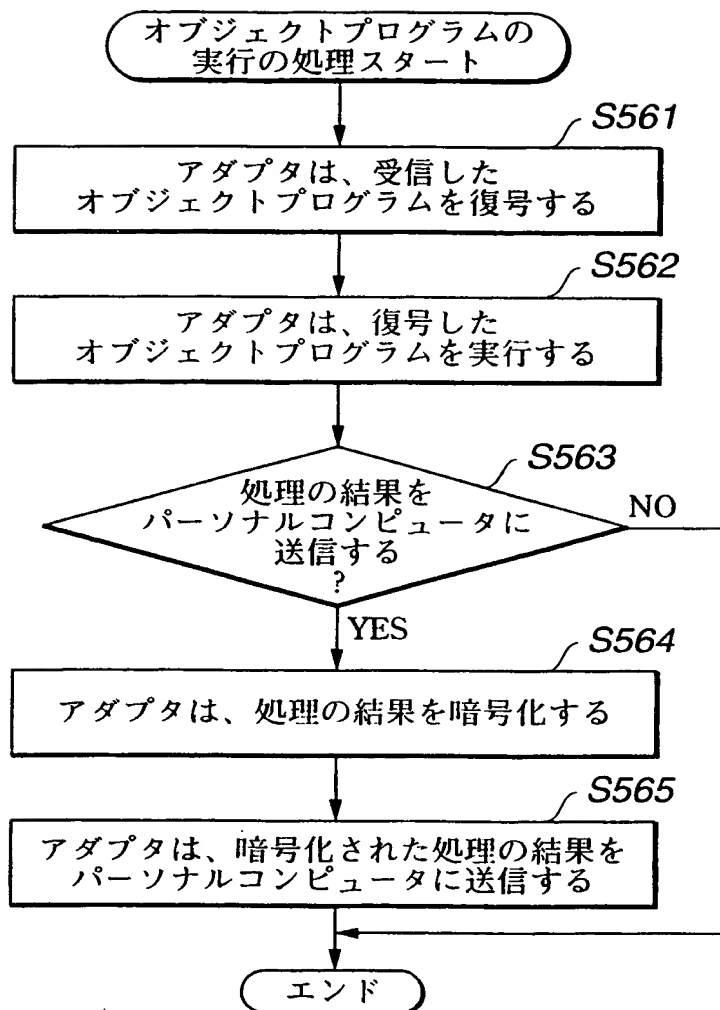


FIG.45

**THIS PAGE BLANK (USPTO)**



45/48

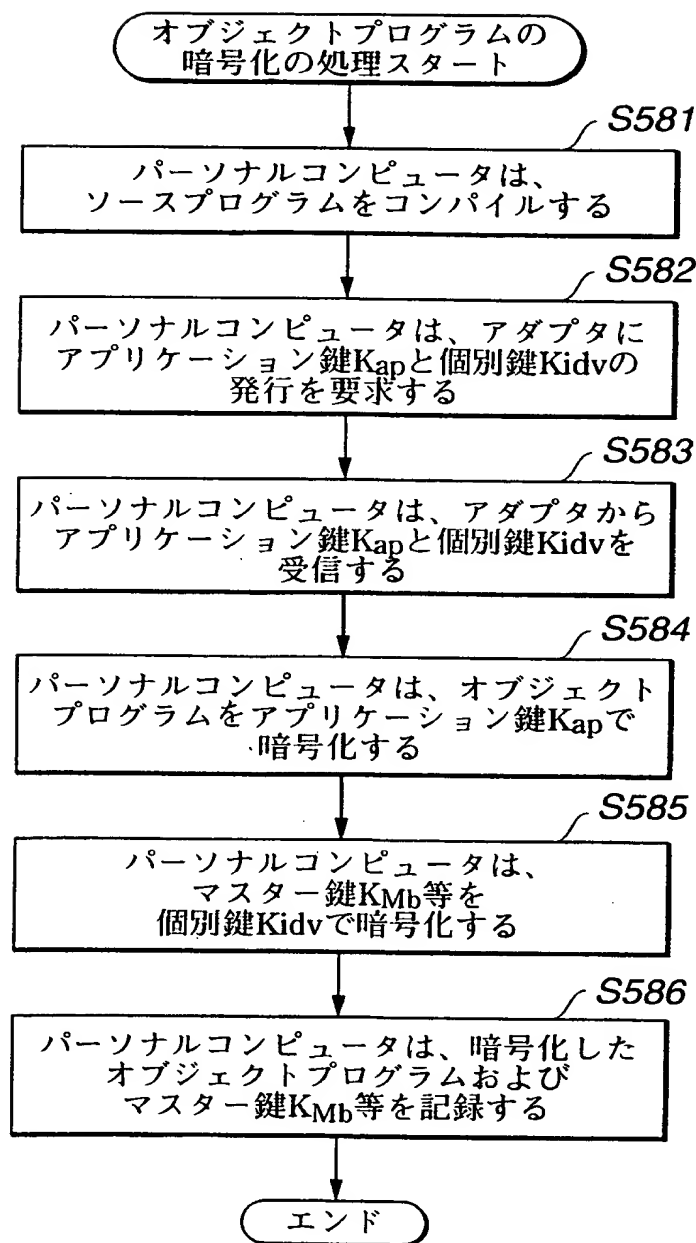


FIG.46

**THIS PAGE BLANK (USPTO)**

46/48

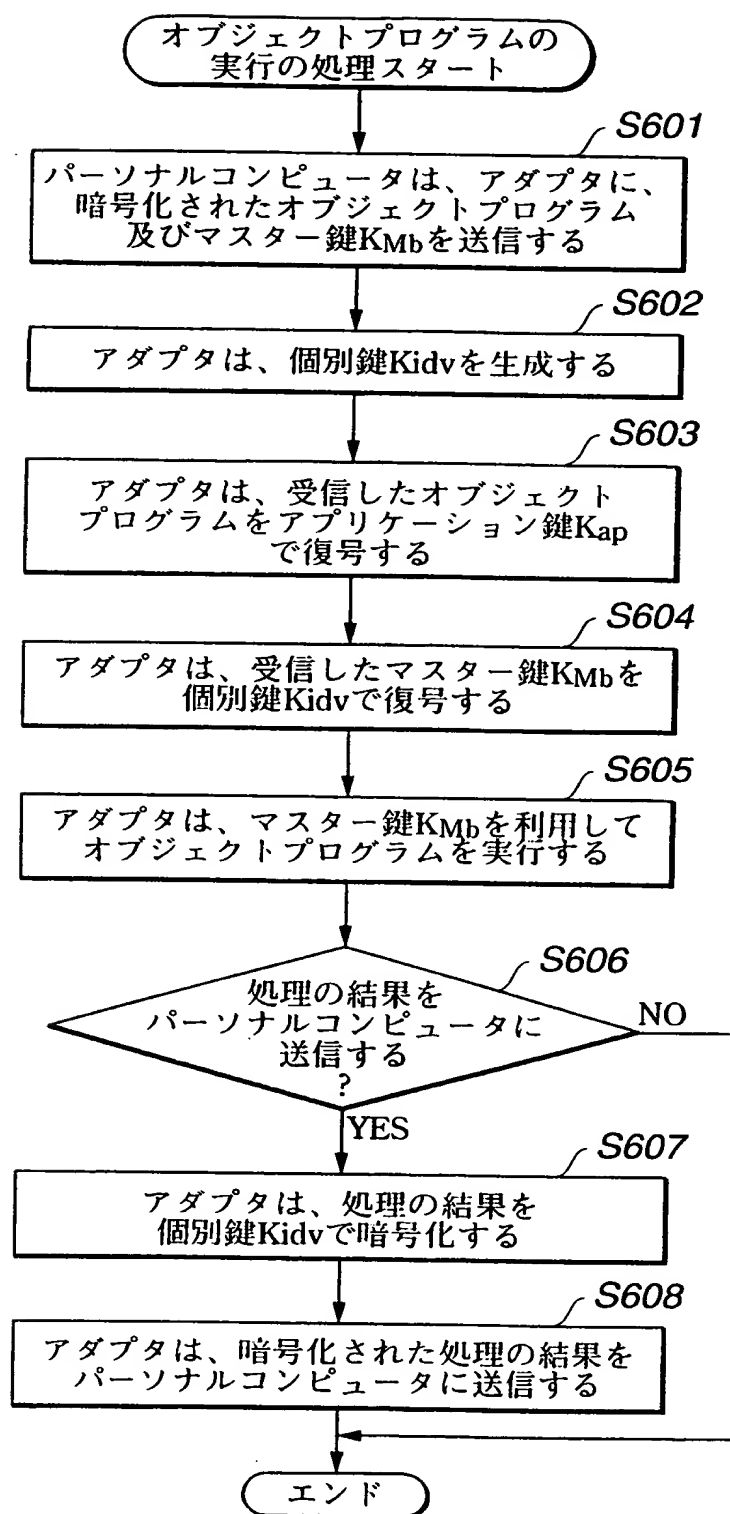


FIG.47

**THIS PAGE BLANK (USPTO)**

47/48

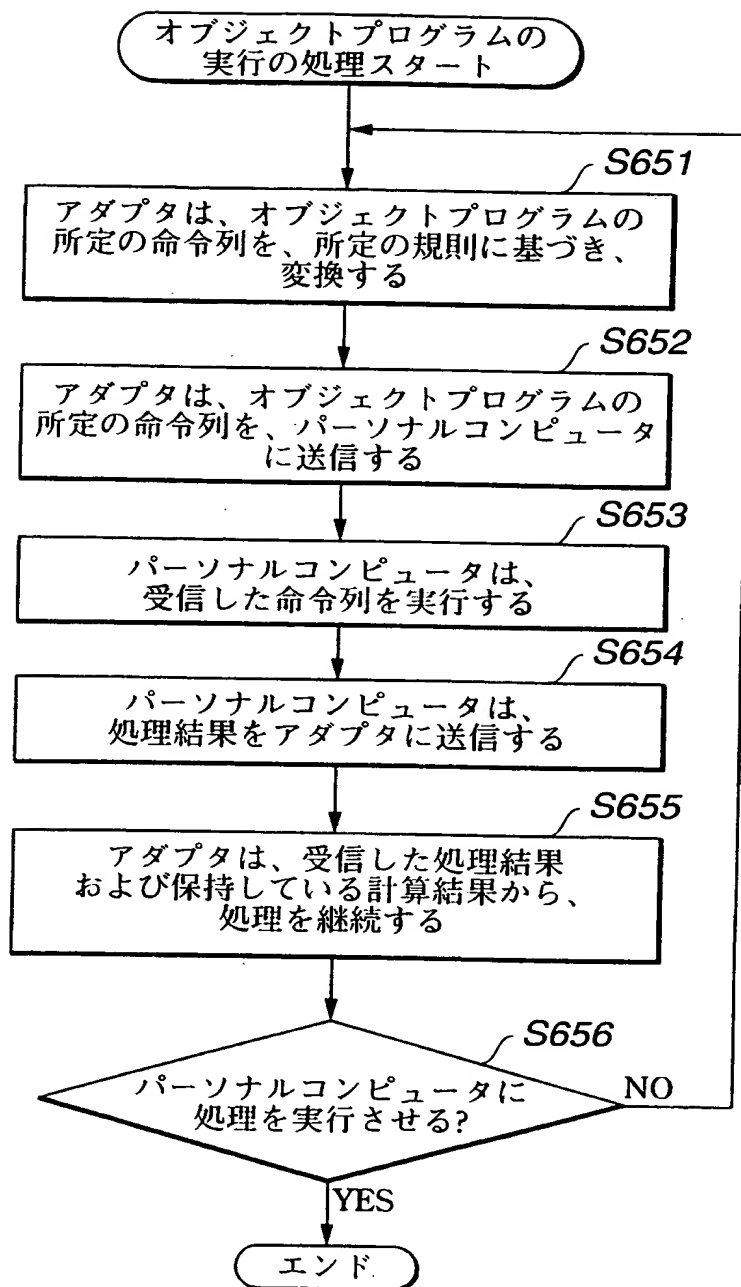


FIG.48

**THIS PAGE BLANK (USPTO)**

48/48

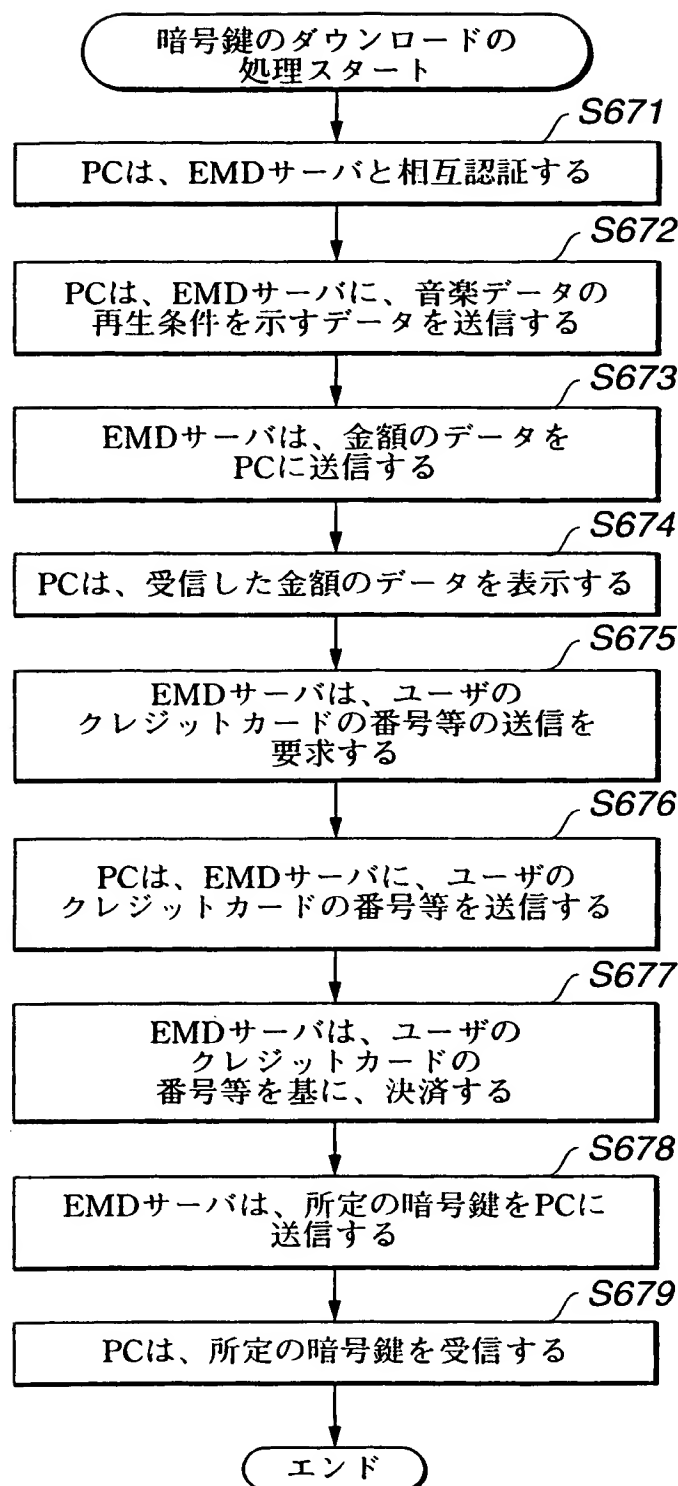


FIG.49

**THIS PAGE BLANK (USPTO)**



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60  
H04L 9/00~9/32  
G09C 1/00~5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG (INSPEC): OpenMG, MagicGate, MemoryStick  
JICST (JOIST): OpenMG, MagicGate, MemoryStick, Copyright, Contents Down Load

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Taro Yoshio, "Digital Chosakuken:Kogata Memory Card de Chosakuken wo mamoru", <i>Nikkei Electronics</i> , No.739, 22 March, 1999 (Tokyo), p.49-53	1-52
X Y	Taro Yoshio, "Ongaku Haishin matta nashi: Seibi Isogu Chosakuken Hogo Gijutsu", <i>Nikkei Electronics</i> , No.738, 08 March, 1999 (Tokyo), p.94-98	11-14 1-10, 15-52
Y	EP, 875815, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 16 & JP, 10-301772, A	1-5, 15-52
Y	EP, 875814, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 22 & JP, 10-301773, A	1-5, 15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO.LTD.), 02 September, 1998 (02.09.98), Full text; Figs. 1 to 9 & JP, 10-304333, A	6-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
21 June, 2000 (21.06.00)

Date of mailing of the international search report  
04 July, 2000 (04.07.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"DVD, Personal Computer ni noru Software Fukugou no Kagi wo nigiru Fusei Copy Boushi Gijutsu no Medo", <i>Nikkei Electronics</i> , No.696, 18 August, 1997 (Tokyo), p.110-119	9-10,15-52
Y	David Aucsmith, "Gyaku Kaiseki ya Kaihen kara Soft wo mamoru Tamper Resistant Software Gijutsu no Shousai", <i>Nikkei Electronics</i> , No.706, 05 January, 1998 (Tokyo), p.209-220	9-10,15-52
Y	EP, 874299, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 32 & JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 41 & JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.), 06 September, 1996 (06.09.96), Full text; Figs. 1 to 87 & JP, 10-512074, A	1-52

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02041

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-5 relate to an information providing apparatus for receiving a program from a program information processing device over a network, encrypting the received program, and transmitting it to information processing device, to an information providing method, and to a program providing medium.

There is no special technical feature common to the inventions of claims 6-52 and those of claims 1-5.

For example, the inventions of claims 6-8 relate to an information processing apparatus for selecting a mutual authentication to be made from among mutual authentications between information processing devices and carrying out the mutual authentication, to an information processing method, and to a program providing medium.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

**THIS PAGE BLANK (USPTO)**

## 国際調査報告

国際出願番号 PCT/JPO0/02041

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int Cl <sup>7</sup> G06F9/06		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int Cl <sup>7</sup> G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60 H04L 9/00~9/32 G09C 1/00~5/00		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2000年 日本国登録実用新案公報 1994-2000年 日本国実用新案登録公報 1996-2000年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語) DIALOG (INSPEC): OpenMG, MagicGate, MemoryStick JICST (JOIST): OpenMG, MagicGate, メモリースティック, 著作権, コンテンツ配信		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	日経エレクトロニクス, 第739号, 22. 3月. 1999 (東京), 芳尾太郎, "デジタル著作権: 小型メモリ・カードで著作権を守る", p. 49-53	1-52
X Y	日経エレクトロニクス, 第738号, 08. 3月. 1999 (東京), 芳尾太郎, "音楽配信待ったなし・整備急ぐ著作権保護技術", p. 94-98	11-14 1-10, 15-52
Y	EP, 875815, A2 (SONY CORPORATION) 4. 11月. 1998 (04. 11. 98) 全文, 第1~16図 &JP, 10-301772, A	1-5, 15-52
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 21. 06. 00	国際調査報告の発送日 04.07.00	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 田川 泰宏 電話番号 03-3581-1101 内線 3545	5B 4236

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	EP, 875814, A2 (SONY CORPORATION) 4. 11月. 1998 (04. 11. 98) 全文, 第 1 ~ 2 2 図 &JP, 10-301773, A	1-5, 15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.) 2. 9月. 1998 (02. 09. 98) 全文, 第 1 ~ 9 図 &JP, 10-304333, A	6-8
Y	日経エレクトロニクス, 第696号, 18. 8月. 1997 (東京), "DVD、パソコンに載る ソフトウェア復号のカギを握る不正コピー防止技術のメド", p. 110-119	9-10, 15-52
Y	日経エレクトロニクス, 第706号, 05. 1月. 1998 (東京), David Aucsmith, "逆解析や改変からソフトを守る タンパ・レジスタント・ソフトウェア技術の詳細", p. 209-220	9-10, 15-52
Y	EP, 874299, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98) 全文, 第 1 ~ 3 2 図 &JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98) 全文, 第 1 ~ 4 1 図 &JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.) 6. 9月. 1996 (06. 09. 96) 全文, 第 1 ~ 8 7 図 &JP, '10-512074, A	1-52

## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-5はネットワークを介してプログラムを情報処理装置からプログラムを受信し、受信したプログラムを暗号化して、前記情報処理装置に送信する構成を有する情報提供装置、情報提供方法およびプログラム提供媒体に関するものである。

一方、請求項6-52については上記の構成とは共通の特別な技術的特徴はない。

たとえば、請求の範囲6-8は情報処理装置間の相互認証を行う際において、1以上の相互認証の手続きから、実行する相互認証の処理を選択し、実行する構成を有する情報処理装置、情報処理方法およびプログラム提供媒体に関するものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**